MANPOWERGROUP

# Policy on Gifts, Entertainment and Sponsorships

ManpowerGroup BeLux
PR/21/0/ENG - 01/08/2022

ManpowerGroup®

# TABLE OF Contents

# I. Introduction

**This Policy is to assist you in determining whether to provide gifts, meals and entertainment, hosting, sponsorships, and travel benefits to third parties, particularly where government officials are involved.** It also sets forth the processes that should be followed. It should be read and understood in conjunction with the ManpowerGroup Anti-Corruption Policy. This policy applies to all employees, officers, members of the Board of Directors and others who act on behalf of ManpowerGroup.

### Government officials may include:

- ✓ Heads of state, ministers, and other political appointees;
- ✓ Civil servants;
- ✓ Other full or part-time employees of government;
- ✓ Private citizens acting in an official capacity;
- ✓ Security personnel (military, police, intelligence);
- ✓ Judges and legislators;
- ✓ Officers and employees of state-owned or controlled enterprises (for example, a state-owned petroleum company or airline); and
- ✓ Employees of other public institutions, including universities, laboratories, hospitals, and the like.

ManpowerGroup's Anti-Corruption Policy strictly prohibits bribery and corruption of any kind in connection with the Company's business. Providing gifts, entertainment, and hosting, as well as sponsorship travel or other activities, can be a legitimate part of doing business. However, these activities can also be considered corrupt benefits in some circumstances and can lead to criminal liability for those involved. In addition, they may be regulated by the locale or country government where the benefits are provided, or restricted by the recipient's organization. This is particularly true where the benefits are received by individuals considered to be government officials under relevant laws. "Government officials" is a broad definition that can also include officials of government owned or controlled companies. In all cases, ManpowerGroup is required to maintain proper internal controls and adequate books and records relating to these benefits.

**The rules and expense limits in this Policy govern your actions with third parties, such as clients, vendors, and government officials. Internal expenditures for gifts meals and entertainment – such as for your colleagues and teams — are not subject to this global policy. However, you are expected at all times to use good judgment, and comply with your local approval process, for such activities.**

Any employee who becomes aware, or suspects, that this Policy has been violated should immediately:

- ✓ Notify their manager or supervisor,
- ✓ Notify the General Counsel or the Global Ethics Compliance Officer, or
- ✓ Report concerns through the ManpowerGroup Business Ethics Hotline

# II. General Rules Applicable to All Types of Benefits

Gifts, meals, entertainment, hosting, and the provision of sponsorships or other benefits, including travel sponsorships, are referred to in this Policy as "Benefits."

## The following rules apply:

1. Benefits are **never** permissible when given to government officials, business partners, clients or prospective clients to influence their actions or decisions in their official or business capacity.]
2. Employees are expected to use good judgment in deciding whether to offer or provide Benefits and should be prepared to identify the legitimate business purpose of the Benefits. The specific sections that follow provide some examples of legitimate activities.
3. All requirements of local law and rules of the recipient's organization should be complied with. Many companies limit the gifts or entertainment their employees can accept and client contracts may impose additional restrictions. Before you provide Benefits to a third party, it is your responsibility to obtain any required ManpowerGroup approvals, and also to confirm that local law, as well as the policies of your recipient, are being observed.
4. This Policy includes Global monetary limits. **Your country might have adopted lower expense limits to reflect local practices.** It is your responsibility to understand and comply with both Global and country-specific requirements.
5. Benefits should **always** be reasonable in amount and appropriate in nature.
6. Certain types of Benefits should never be provided. This includes cash Benefits, Benefits associated with illegal activity or activities that may harm the Company's reputation, such as escort services, adult entertainment venues or gambling.

7. Appearances should be considered. Benefits most people would consider lavish or extravagant, or are of a personal character (for example, jewelry or luxury goods), tickets to premium events or trips to leisure destinations, should generally not be provided.

8. Benefits, such as gifts, given when there are pending business or contracting decisions with the recipient that could benefit ManpowerGroup may also create appearance issues, and should generally not be provided.

9. The frequency of Benefits to particular recipients should be monitored. Even relatively modest benefits, such as meals, when provided frequently, can create legal or appearance issues, and should be avoided.

10. The aggregate value of Benefits to particular recipients should also be considered. If the total value of gifts, meals and entertainment provided to a particular individual over the course of a year exceeds **$250**, caution should be used before providing further Benefits to this individual.

11. The use of personal funds to provide Benefits is prohibited.

12. Benefit-related expenses must be accurate and complete and appropriately documented. Appropriate documentation includes receipts for expenditures, information about any attendees and beneficiaries (including name and place of employment), and explanation of the business purpose.

13. All expenditures for Benefits must be approved as set forth in Section VII below.

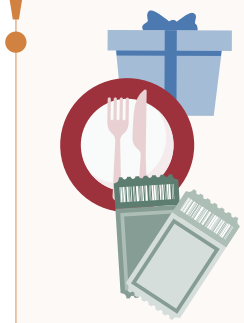
14. Operations that believe the circumstances of their business require different thresholds or approaches than what is set forth in this policy should discuss their needs with the Global Ethics Compliance Officer.

# III. Gifts

All gifts should be appropriate to the occasion, reasonable in amount, and provided only as a courtesy or token of esteem. Gifts should not be given to influence the selection of the Company's services, or to influence or induce any action of a government official or business partner. **ManpowerGroup has a global gift limit of USD $150**. You cannot exceed this global limit without prior written approval. To obtain approval, please refer to the Approvals chart in Section VII. In addition to the global limits, Country-specific expense limits for gifts have been set by each country manager. Check your country-specific limit before providing any gift.

In addition to the guidance in Section II, the following guidelines apply to **gifts** given to Government officials, business partners, clients or prospective clients:

- ✓ Gifts should be given openly and transparently, consistent with the occasion. If you do not feel comfortable doing so, that is a sign of a potential issue.
- ✓ Local custom and practice in some locales may be different and should be taken into account.
- ✓ Cash and cash equivalents, such as gift certificates, traveler's checks, mobile phone top-up units, and checks, are never permissible gifts.
- ✓ Gifts to offices or groups that are intended to be shared with colleagues (for example, food baskets), are preferred over gifts to individuals.
- ✓ Particular care needs to be exercised with gifts to procurement officers or others who have the authority to award contracts to the Company. Gifts that are given when contracting decisions are pending may create the appearance of an improper intent to influence and should be avoided.
- ✓ Gifts of items for personal use or for family members or friends of government officials or business partners are less appropriate than Company promotional items, but may sometimes be appropriate (for example, flowers or a "hostess gift" when visiting someone's home for a meal)



**As long as the gift is reasonable, examples of appropriate gifts include:**

- ✓ Gifts to celebrate holidays that are commonly associated with gift-giving, including Christmas, Chinese New Year, and other similar events.
- ✓ Gifts to commemorate specific events, such as a business anniversary, closing of a business transaction, retirement, or the like.
- ✓ Gifts of promotional items engraved with the Company's logo, such as glassware, desk accessories, pens, coffee mugs, shirts, hats, etc., generally are appropriate gifts.

# IV. Meals & Entertainment

As used in this section, meals and entertainment includes both traditional restaurant meals, as well as cultural and sporting events, both in-person or virtual, where we might purchase admission tickets and related food and beverages. Note, meals or entertainment that are part of sponsored travel are covered in Section V below, Travel. **ManpowerGroup has a global meals and entertainment limit of USD $200**. You cannot exceed this global limit without prior approval. To obtain approval, please refer to the Approvals chart in Section VII. In addition to the global limits, Country-specific expense limits for meals and entertainment have been set by each country manager. Check your country-specific limits before providing any meals and/or entertainment.

### Examples of legitimate meals and entertainment include:

- ✓ Lunch incidental to a business meeting with a client.
- ✓ Dinner to commemorate the launch of a new business relationship.
- ✓ Inviting a business partner or client to join an employee at a soccer match. Note, the total event expenses, including tickets and any food and/or beverage provided should not exceed the global limit.
- ✓ You have a two-day planning meeting with a client or prospective client. On the second day, you organize a closing dinner cruise.

In addition to the general guidance in Section II above, the following guidelines apply to the provision of **meals and entertainment** to Government officials, business partners, clients or prospective clients:

- ✓ Business meals should be infrequent, consistent with country norms and local business practices, and never extravagant.
- ✓ ManpowerGroup Employees should select venues for meals and entertainment that will fall within this Policy. If you leave it to the person you are entertaining to select the venue, you may create a situation where you will be unable to meet this Policy. Plan in advance and avoid difficult and embarrassing situations!
- ✓ Family members or friends of a government official, business partner, client or prospective client may not attend a meal, sporting event or entertainment activity at Company expense, unless the spouses or friends of ManpowerGroup Employees are also attending, or advance approval has been obtained from the Global Ethics Compliance Officer.
- ✓ Entertainment can be part of a legitimate business gathering, provided the primary purpose of the gathering is business or business development. Stand-alone entertainment outings with no related business purpose, such as a golf weekend, are not generally appropriate business entertainment and require specific advance approval from the Global Ethics Compliance Officer.
- ✓ A Company employee or representative should attend any sporting events or entertainment activities with the government official, business partner, client or prospective client. For example, giving tickets to a sporting event so the individual can attend the event alone or with guests of their choosing is generally not appropriate.
- ✓ Where possible, payment for hosted meals and entertainment should be made by ManpowerGroup Employees directly to service providers.
- ✓ In those more unusual circumstances where reimbursement to a Government official or business partner for meals or entertainment is appropriate, the reimbursement must be supported by appropriate receipts reflecting the nature and amount of the expense being reimbursed.

# V. Travel Sponsorships

Generally, government officials, business partners, clients or prospective clients are expected to pay the costs of their own travel. However, there may be certain circumstances where the Company pays the travel expenses for a government official, business partner, client or prospective client to visit a company business location, for a joint meeting, or for some other appropriate business purpose. Travel sponsorship costs may include transportation, accommodation, and meals, as well as other incidental costs. Travel sponsorship by the Company can involve significant expenditures of funds and require approval. To obtain approval, please refer to the Approvals chart in Section VII.


**Examples where the Company can pay the travel costs include:**

- ✓ A board meeting of a joint venture where the Company's partner is a state enterprise.
- ✓ A contract with a client requires you to pay for travel of personnel for training purposes.
- ✓ A potential client wants to observe how services are provided at a particular locale.
- ✓ A visit to the Company's headquarters to understand ManpowerGroup's capabilities.

In addition to the general requirements in Section II above, the following guidelines apply to the provision of **travel sponsorships** to government officials, business partners, clients or prospective clients:

- ✓ All sponsored travel should involve a legitimate business purpose. Travel sponsorships that are purely for leisure or entertainment will not be approved.
- ✓ Payments in the form of a per diem for persons whose travel is being sponsored, e.g., cash payments or "walking around money," will generally not be approved.
- ✓ Where possible, payment of travel sponsorship expenses should be made directly to the service provider, e.g., airline, hotel, restaurant.
- ✓ If reimbursement for sponsored travel expenses is appropriate, the reimbursement must be supported by appropriate receipts reflecting the nature and amount of the expense
- ✓ Generally, the sponsored individuals' company, agency or organization, rather than Manpower Group, should select the specific individuals whose travel will be sponsored.
- ✓ Sponsored individuals should be prepared to demonstrate that they have received all internal approvals to enable them to travel.
- ✓ No family members or friends may accompany the government official, business partner, client or prospective client on the trip at the Company's expense, unless the family and/or friends qualify to receive such hosting in their own right.

# VI. Event Sponsorships

Event sponsorships can take various forms, for example, where the Company sponsors an exhibition, activity, program, or the like. Event sponsorships typically allow the Company to promote its services or to gain visibility and goodwill. Events that are closely connected with government officials, business partners, clients or prospective clients (for example, the sponsorship is requested by a government official, or the organization to be sponsored is known to be linked to a government official or an immediate family member of the official), present special issues, as do sponsorships made in the context of a pending contract. To obtain approval in such situation, please refer to the Approvals chart in Section VII.

In addition to the general requirements in Section II above, the following guidelines apply to **event sponsorships** benefitting Government officials or business partners:

- ✓ Event sponsorships should have as their primary purpose the promotion of the Company's services, good corporate citizenship, or other legitimate business justification.
- ✓ The Business Unit seeking to sponsor the event should conduct due diligence on event organizers and persons seeking the Company's sponsorship and the results documented and retained. Where possible, payment should be made directly to the event organizer. Sponsorships should not be paid in cash.
- ✓ Company employees should take steps to verify that sponsorship funds are used for the intended purpose, and that the Company receives the agreed benefits in return for the sponsorship.
- ✓ Any travel in connection with the event sponsorship must comply with the requirements of the Travel Section of this Policy, set forth in Section V.
- ✓ Gifts provided in connection with the event sponsorship must comply with the requirements of the Gift Section of this Policy, set forth in Section III.

# VII. Authorizations and Approvals

The chart below outlines the approval requirements under this Global Policy. Don't forget to comply with any local limits or approval requirements.

## Gifts, Entertainment, and Sponsorships Approvals

| Type of Benefit Provided | Approval Is Required For: |
|---|---|
| Gifts | Gifts exceeding **$150** per recipient. |
| Meals and Entertainment | Meals and entertainment exceeding **$200** per recipient. |
| Stand-alone entertainment outings with no related business purpose | All outings. |
| Travel sponsorships | All travel sponsorships. |
| Sponsoring events that are closely connected to government officials, business partners, clients, or prospective business partners or clients | All events. |

## Approval Process

All requests for approval should be emailed to:

giftsandentertainment.authorization@manpowergroup.com.

Please include details regarding the proposed expenditure, including the name, title and affiliation of proposed attendees, budget, service providers. You must also state the business purpose.

The Global Ethics Compliance Officer will consider your request. All approvals will be made in writing. If an approved expenditure changes materially from the proposal provided (e.g., if the actual budget significantly exceeds the proposed budget, or if the attendees change), re-approval is required.

## Record-Keeping

You must retain records of expenditures. Any submitted expense reports must reflect, in writing, the names, titles and affiliations of the attendees and the business purpose for incurring the expenditure.

## VIII. Administration and Inquiries

The General Counsel, **Richard Buchband**, oversees compliance with this Policy and the Company's anti-corruption program. Under his direction, **Shannon Kobylarczyk**, Global Ethics Compliance Officer handle inquires and approvals.

If you have questions, please contact Shannon at **414.906.7024** or write to our team at ethics.training@manpowergroup.com or generalcounsel@manpowergroup.com.

ManpowerGroup

# ESG/SUSTAINABILITY

ENVIRONMENT

## ENVIRONMENT

"Now is the time for climate action."

*#TheChangeStartsWithYouAndMe*


### OUR COMMITMENT

**ManpowerGroup** is committed to the fight against global warming. In 2021, our climate targets were validated by Science Based Targets (SBTi), the leading authority on climate action in the world of business.

**Our ambition is to reach net zero emissions no later than 2045 and in this transition we have committed ourselves, by 2030, to:**

- **reduce direct emissions from our operational activities by 60%** (Scope 1 & 2 - energy and electricity consumption in buildings, company cars etc.)
- **reduce value chain emissions by 30%** (Scope 3 - waste management, travel, mobility, suppliers).

**ManpowerGroup Belgium** shares the same ambition.
To achieve our global strategy, we have set the following objectives:

## ENERGY

- 100% renewable energy for our offices by 2030.
- Progressive transition of our branch network to low-carbon footprint buildings.
- Decrease our energy consumption

## MOBILITY

- Zero $CO_2$ emissions from our company cars by 2030.
- Implementing actions to decarbonize our commuting (mobility plan, flexible working hours, hybrid working models, minimizing business travel).

## ZERO PAPER / ZERO WASTE / RECYCLING

- 95% of our external documents in electronic form by 2024 and reduce internal document printing moving towards 'Zero Paper'.
- 100% Sorting & Recycling: procedures in place to ensure optimal reduction and sorting of internal waste, as well as recycling of materials (office furniture, IT equipment, electrical equipment, ink cartridges, etc.)

## SUSTAINABLE PROCUREMENT

- Use of sustainable products in the daily running of the company (office supplies, bags, promotional materials, cups, etc.)
- Imposing environmental standards on our suppliers.

We raise awareness of environmental issues among all stakeholders.

All ManpowerGroup employees contribute to the achievement of our climate objectives by adopting eco-responsible behaviour on a daily basis.

*'The Change Starts With You And Me'*

**Sébastien Delfosse**
Managing Director ManpowerGroup BeLux

ManpowerGroup BeLux
PR/18/3/ENG - 01/10/2025

ManpowerGroup

# ESG/SUSTAINABILITY

SOCIAL DIALOG

## SOCIAL DIALOG POLICY

"We are convinced that maintaining a healthy social climate is essential for ensuring a healthy economic climate."

We are committed to building trusting relationships with our social partners and to respecting the role of trade unions within their legal remit.

The Human Resources department of ManpowerGroup BeLux, in close collaboration with the Head of Social Relations and the Head of the Legal department, manages and leads ManpowerGroup's professional, trade union and institutional relations.

They work with the:

- management of the social calendar and meetings of staff representative bodies;
- negotiations with representative trade unions:
- the individual and collective management of staff representatives;
- social elections.

ManpowerGroup BeLux

ManpowerGroup BeLux
PR/18/3/ENG - 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.

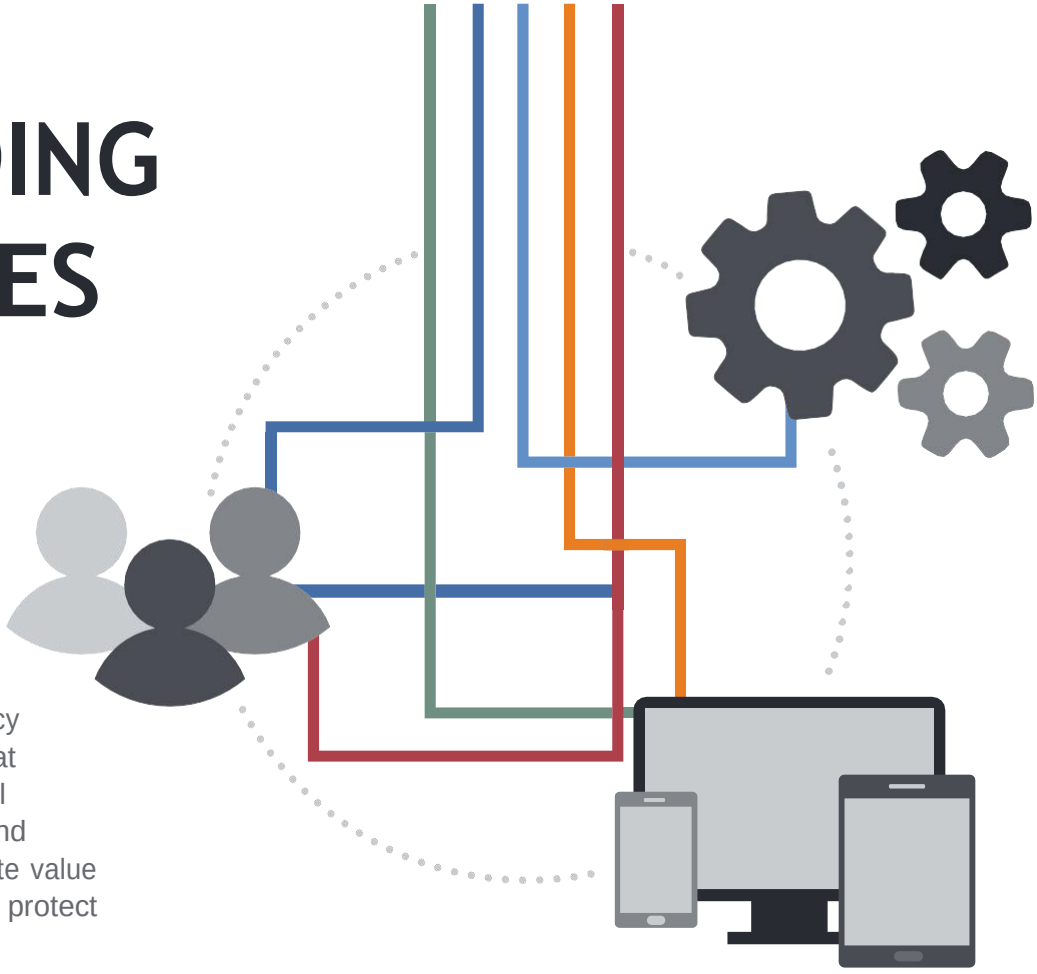
*"As technology evolves and we adopt new tools and expand our use of data and analytics to deliver more value to clients and candidates, we are committed to being good stewards of the information entrusted to us. Managing our information security is vital to ensuring trust and transparency with our employees, 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.

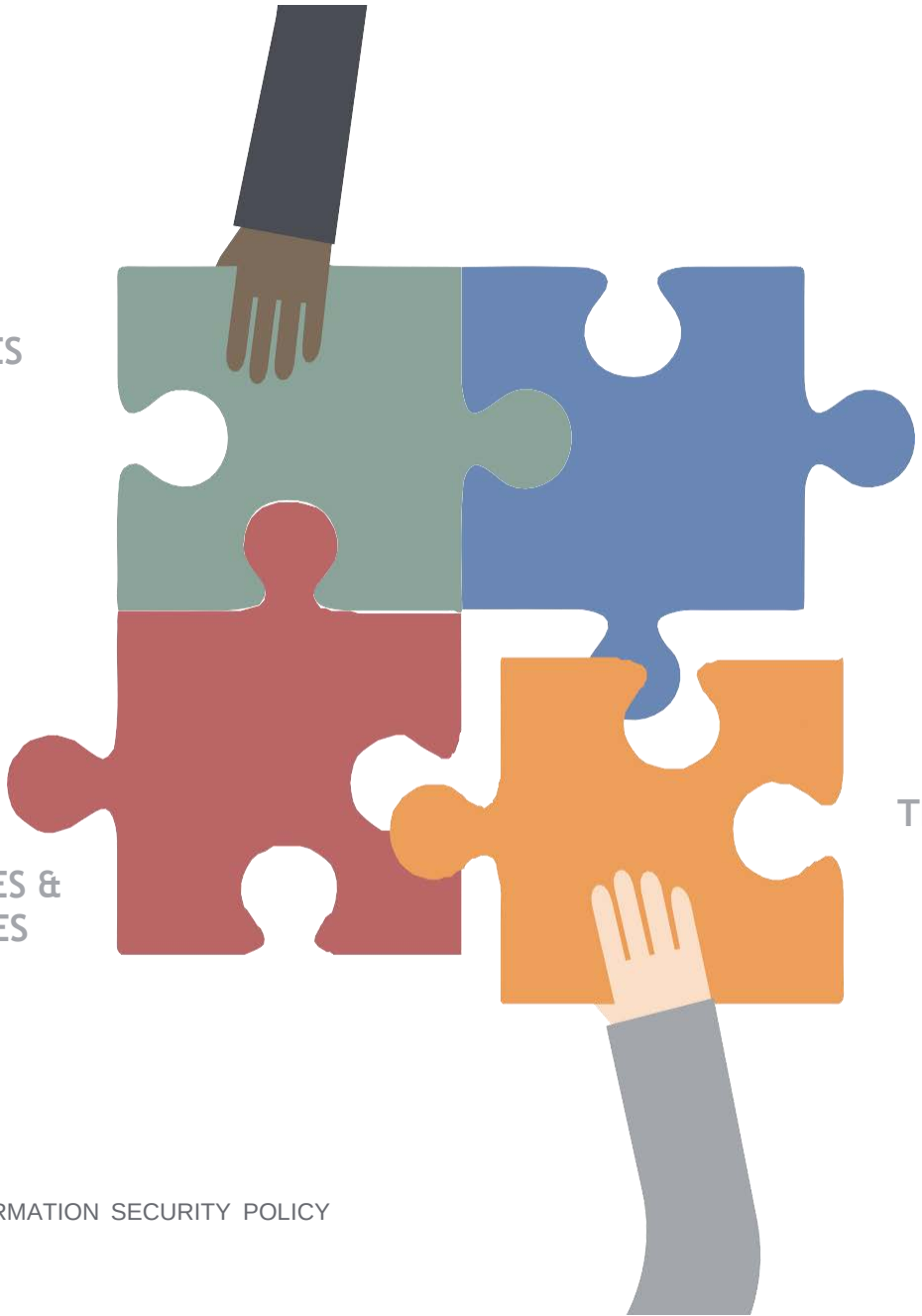
## TECHNOLOGY

- 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.

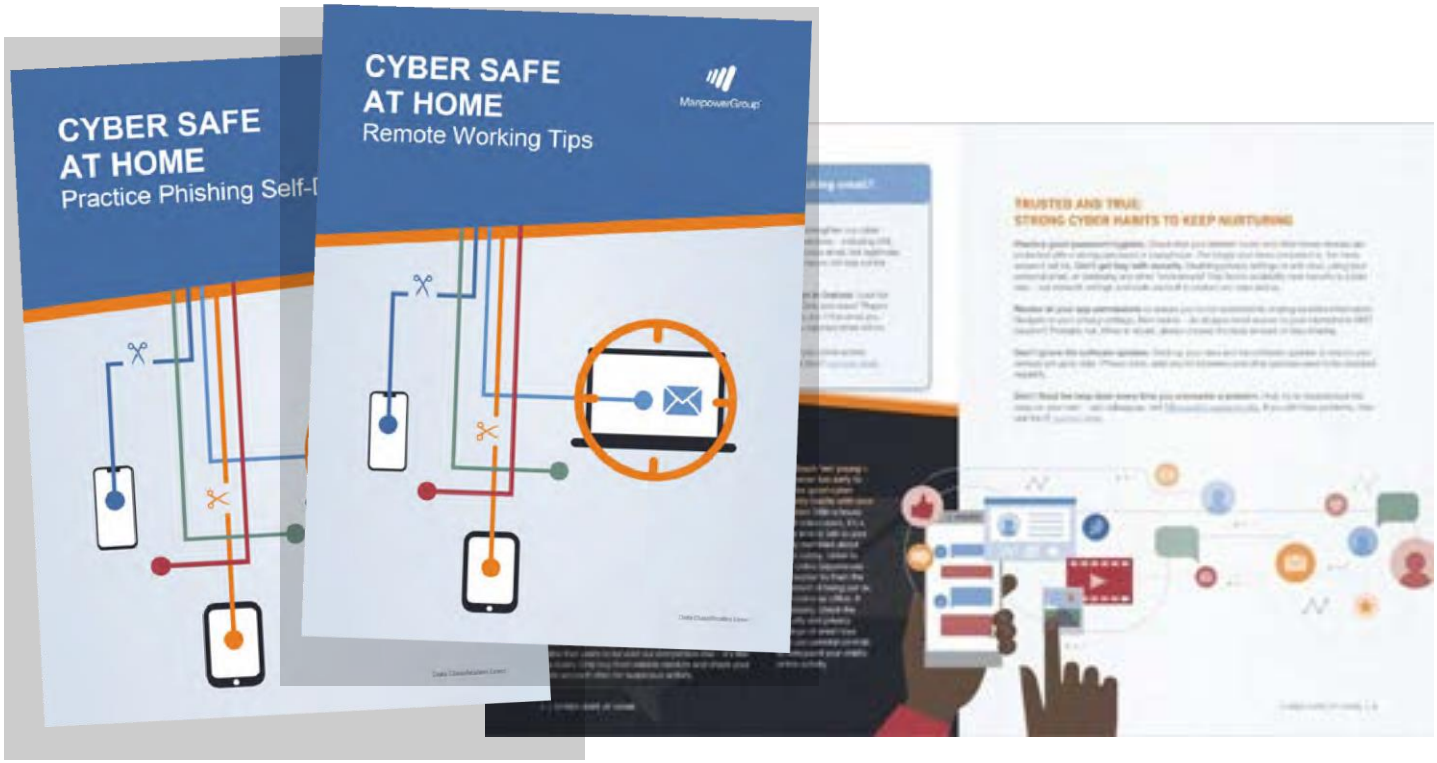
Our talented team dedicated to information security and data privacy has increased in size significantly over recent years. Our people are strategically positioned at the global, regional and local market levels to provide consistent policies, processes and technology solutions. Our highly trained staff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

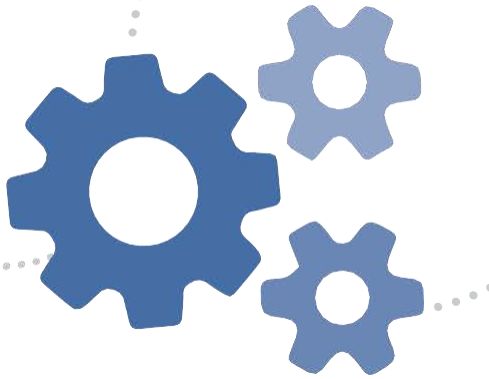



## Embedding Security into our People & Culture Practices

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

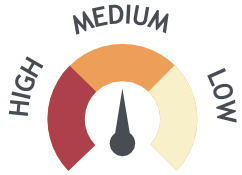
### Analyzing Risks

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

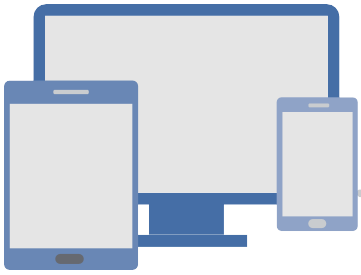
To safeguard our information assets, access is limited to authorized, business-justified entities with a “need to know.” We have taken thorough measures to prevent the inappropriate use of access credentials:

- 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

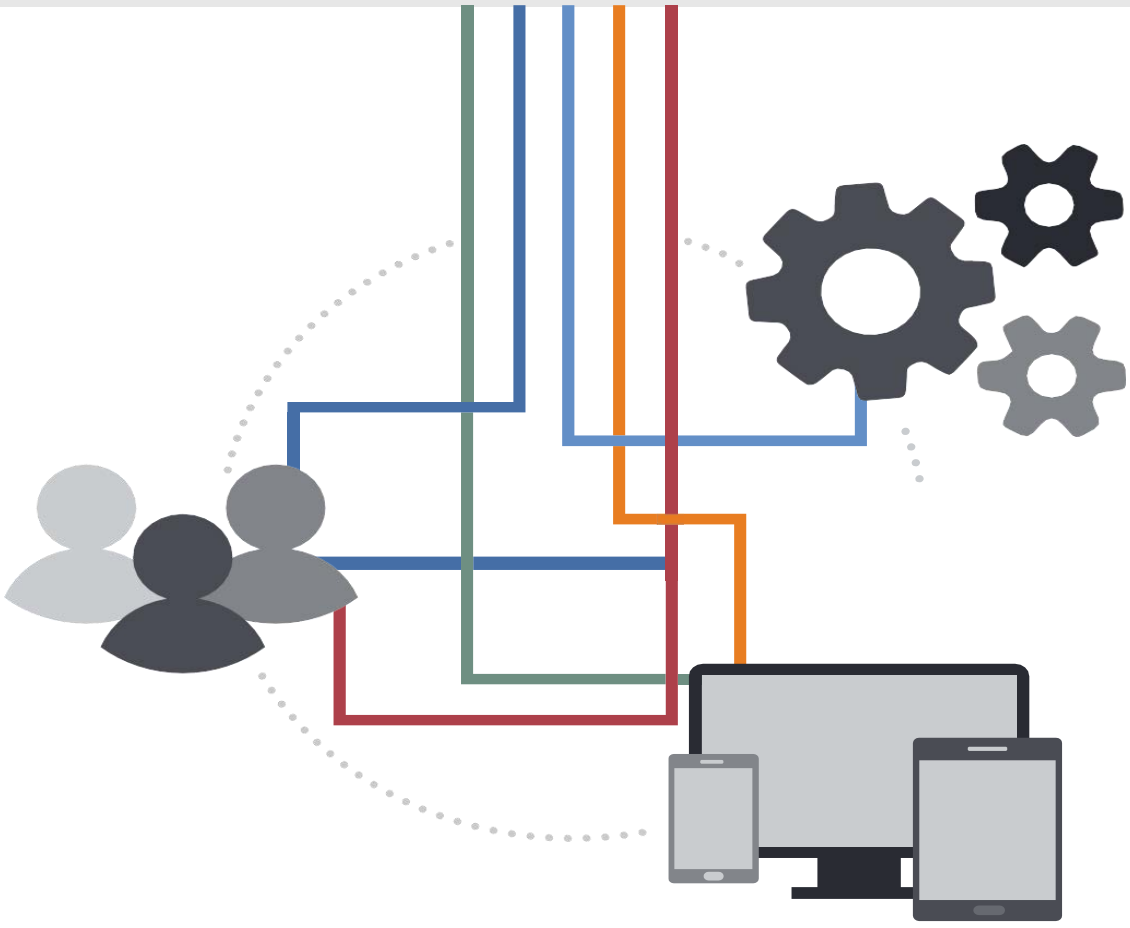
We protect from malicious code execution (Malware) through activities including:

- 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

# ESG & SUSTAINABILITY POLICIES

**There is more information on ManpowerGroup's sustainability strategy here:**

**> Worldwide: manpowergroup.com**

**> For Belgium: manpowergroup.be**

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

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