Information Security and Data Privacy

Protecting and respecting the information entrusted to us

Why This Matters

The world of work is becoming increasingly digital and data-driven, and the frequency and sophistication of cyber-crimes is rising. Our Center of Excellence in People Analytics, Assessment and Innovation is responsible for sourcing and piloting new innovations that drive meaningful impact for our business, including assessments, AI and machine learning and new platform technology. As a result, managing our information security and knowing how to respond to emerging tech's ethical and equity concerns has never been more vital.

We must articulate our commitment to being good stewards of the information entrusted to us and take responsibility to be vigilant and educate our people seriously. In the long tail of COVID-19, the mass migration to remote working and rapid digitization of processes requires even greater prioritization of information security and privacy to protect our data and workers while ensuring trust and transparency with our employees, clients and partners.

Proud of Our Progress: Where We Are Today

Leadership at the Top

Under the direction of the Chief Information Security and Chief Privacy Officer (CISO/CPO), responsibility for our global security program resides at the highest levels of executive leadership, reporting to the Chief Financial Officer. The CISO/CPO meets quarterly with the Audit Committee of the Board of Directors to review and discuss security strategy and progress around our investments. All members of the Executive Leadership Team are included in all cyber training and phishing awareness campaigns alongside the whole organization.

In addition, to ensure our innovations are built on our strong ethical foundation, we look to our Ethical AI Taskforce, led by our General Counsel, Chief Innovation Officer and Chief Information Security Officer, to review and map innovations for the following priorities: data privacy, cyber security, human oversight, explainability, technical robustness and legal accountability.

Global Standards and Frameworks

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 on our corporate website, the Code is shared with every employee and all of our stakeholders around the world.

Our Global Privacy Policy describes the types of personal information we collect from candidates, associates and clients, including how we use it, with whom we share it and the rights and choices available to individuals regarding our use of their information.

Maintained at the country level, employee (internal staff) privacy policies align with our global standards and comply with all local laws and regulations. A holistic global privacy program was established to ensure that the personal identifiable data of candidates, associates, business partners and employees is processed in ways to minimize risks toward individuals.

We have established a comprehensive global information security framework, aligned with the internationally recognized ISO 27001 standard, which all of our operations around the world are required to adopt. All of the data centers that support our key market operations (80% of our business) are certified to ISO 27001. In addition, several of our largest country operations (representing 39% of worldwide revenues) also maintain ISO 27001 certification for their local information security management systems.

Managing Risk, Protecting Individuals and Organizations

Keeping information safe requires constant risk assessment. Our Global Risk and InfoSecurity Program (GRIP) is an organization-wide framework that combines people, processes and technology to reduce risk, create value for our clients and ensure the data people entrust to us is protected.

To ensure we are prepared to respond to incidents and effectively neutralize threats, our InfoSecurity and Internal Audit Teams work with an independent third party to conduct Red Team exercises that simulate security attacks against our environment on an annual basis. Our systems are continually tested for vulnerabilities through additional penetration testing and automated scanning tools and services.

Staying Secure: Training and Maintaining Awareness

The frequency and sophistication of cybercrimes are rising, and we take our responsibility to be vigilant and educate our people seriously. We conduct awareness campaigns on an ongoing basis, including digital training courses and email phishing exercises while also requiring annual training for all our employees on data protection, privacy and information security. It's important that we also make it easy for our employees to report concerns through phishing alarm technology integrated with our email system as well as our Information Security Incident Management Policy, which clearly outlines the communication and escalation process for privacy-related events.

We regularly refresh training to address emerging risks or changes in regulations. For example, we enhanced our data protection, privacy and cyber security training in anticipation of the European Union's General Data Protection Regulation, the California Consumer Privacy Act and India's Personal Data Protection Bill — educating and empowering every individual to take responsibility for information security and privacy.

Reporting: A Critical Line of Defense

Employees play a critical role in identifying potential issues. Staff are educated on how to report suspicious activities in their workplace environment or the technology they use. Seamless security integration enables staff to report suspected phishing emails with one click, and our Global Ethics Hotline is available anytime from anywhere, for anyone to report issues or seek guidance. Issues reported via the hotline are reported to the Audit Committee of the Board of Directors.

Through our enhanced and targeted awareness efforts, employee engagement, resilience to social engineering and overall awareness continues to demonstrate measured improvement year on year.

Expanding Our Team, Deepening Our Capabilities

The centralization of our information security and data privacy governance, operations and thought leadership has led to greatly improved security capabilities and maturity enterprise-wide, allowing for rapid deployment of future capabilities. Our cybersecurity program has been assessed by an independent third party over the last three years and has shown measured capability and maturity improvement year after year. This trend is expected to continue for the foreseeable future.

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 ensure consistent policies, processes and technology exist in all locations, all of whom are highly trained with certifications including CISSP, CISM, CISA, CRISC, CQA, Security+, CSCP, CIPM and CIPP/E.

Data Subject Rights and Consent

Data subjects and consumers are transparently informed about how ManpowerGroup manages their data and what the purpose and data retention periods are. Purpose is clearly limited, and retention periods are aligned with legal requirements. Data subjects and consumers can easily execute their rights, including the right to access, rectify and delete their data. Consent and opt-out and opt-in mechanisms are implemented in a consistent and clear manner to allow the individuals to make informed decisions.

Cyber Safe in a Hybrid Workplace

In the very early phases of the COVID-19 health crisis, we swiftly shifted to remote working, even ahead of government lockdowns, in order to ensure our PeopleFirst priority and the safety of our employees, associates, clients and communities. More than 80% of our staff migrated to remote working over a period of 10 days, with data security maintained as a top priority.

With over 20,000 staff using new technology in new locations, we recognized the need to help our people exercise even greater vigilance and created Cyber Safe at Home, an upskilling series to increase our cyber awareness while working from home. The program included guidance on safe, effective use of collaboration tools (our own and others), staying alert to phishing attacks, security tips unique to COVID-19 and all-around good online security habits for work and home use.

With a hybrid workforce now in place, we continue to provide ongoing Cyber Safe at Home guidance.

External Recognition

In recognition of our cyber security approaches, we were recognized as a CS050 award winner. The CSO50 awards recognize security projects that demonstrate outstanding thought leadership and business value.