INFORMATION SECURITY AND DATA PRIVACY

PROTECTING AND RESPECTING THE INFORMATION ENTRUSTED TO US

Why This Matters

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 and partners. At the same time, the frequency and sophistication of cyber-crimes are rising and we take our responsibility to be vigilant and educate our people seriously. In the wake of COVID-19, the mass migration to remote working and rapid digitisation of processes requires even greater prioritisation of information security and privacy.

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 programme 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, and all members of the Executive Leadership Team are included in all cyber training and phishing awareness campaigns alongside the whole organisation.

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 stakeholders around the world.

Our Global Privacy Policy describes the types of personal information we collect from candidates, associates and clients, how we use it, with whom we share it, and the rights and choices available to individuals regarding our use of their information. Employee (internal staff) privacy policies, maintained at the country level, align with our global standards and comply with all local laws and regulations.

We have established a comprehensive global information security framework, aligned with the internationally recognised ISO 27001 standard, which all of our operations around the world are required to adopt. Several operations in key markets, including France, Germany, India and Spain, are externally certified to these standards, as are a majority of our data centre partners.

MANAGING RISK, PROTECTING INDIVIDUALS AND ORGANISATIONS

Keeping information safe requires constant risk assessment. Our Global Risk and InfoSecurity Program (GRIP) is an organisation-wide framework that combines people, process 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 neutralise 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 policies and procedures designed to keep information safe also depend on people to execute them. That's why we roll-out regular employee awareness programmes including annual online training, quarterly phishing exercises and company-wide Cyber Week intensive awareness campaigns, offering daily bite-size training, instructor-led seminars, team activities and security-related quizzes and competitions.

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 DEFENCE

Employees play a critical role in identifying potential issues. Through our awareness training, staff are educated on how to report suspicious activities they may witness in their workplace environment or in 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 centralisation of our information security and data privacy governance, operations and thought leadership has led to greatly improved security capabilities and maturity enterprise-wide, and allows for rapid deployment of future capabilities. Our cybersecurity programme 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, and all are highly trained with certifications including: CISSP, CISM, CISA, CRISC, CQA, Security+, CSCP, CIPM and CIPP/E.

Cyber Safe at Home During COVID-19

In the very early phases of the COVID-19 health crisis, we swiftly shifted to close offices and move 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 recognised 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 programme included guidance on safe, effective use of collaboration tools – our own and others – as well as staying alert to phishing attacks, security tips unique to COVID-19, and all-around good online security habits for work and home use.