MANPOWERGROUP'S INFORMATION SECURITY POLICY

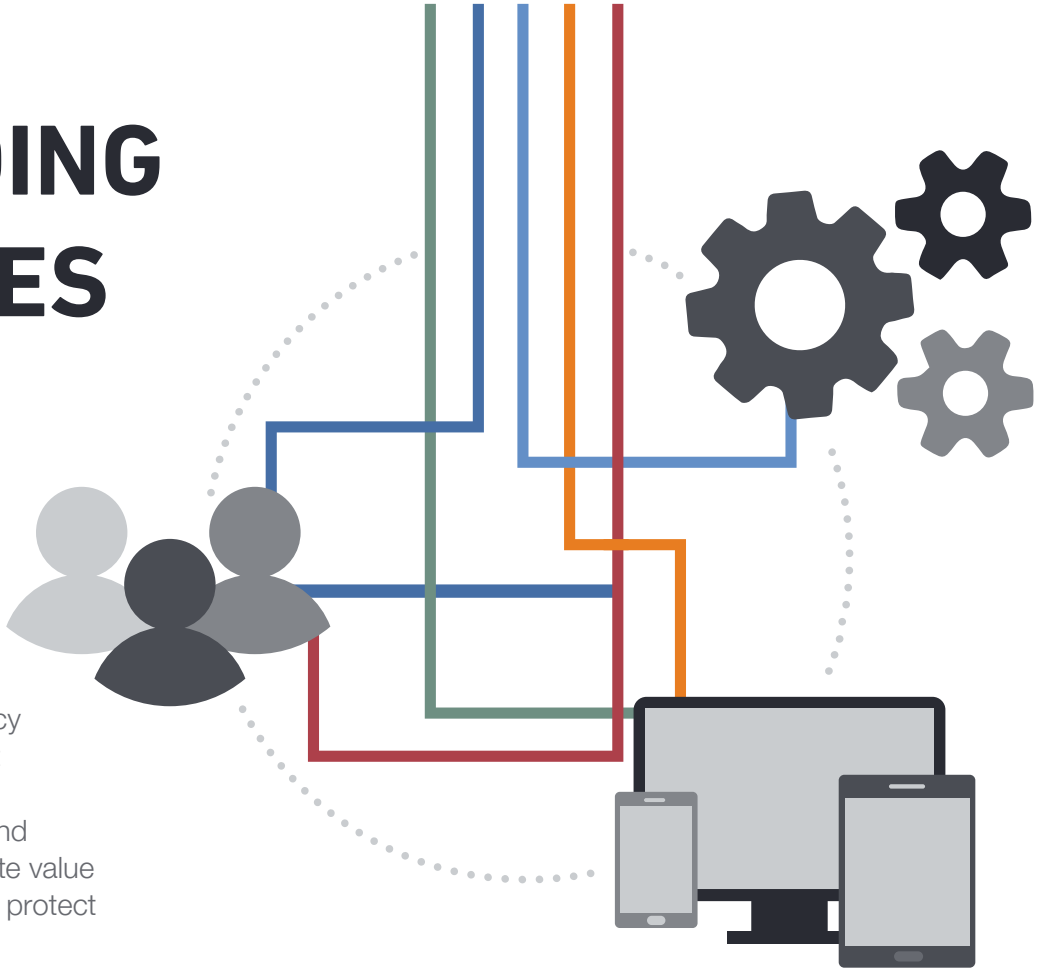
TODAY'S CONTEXT: RAPID DIGITAL TRANSFORMATION

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

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.

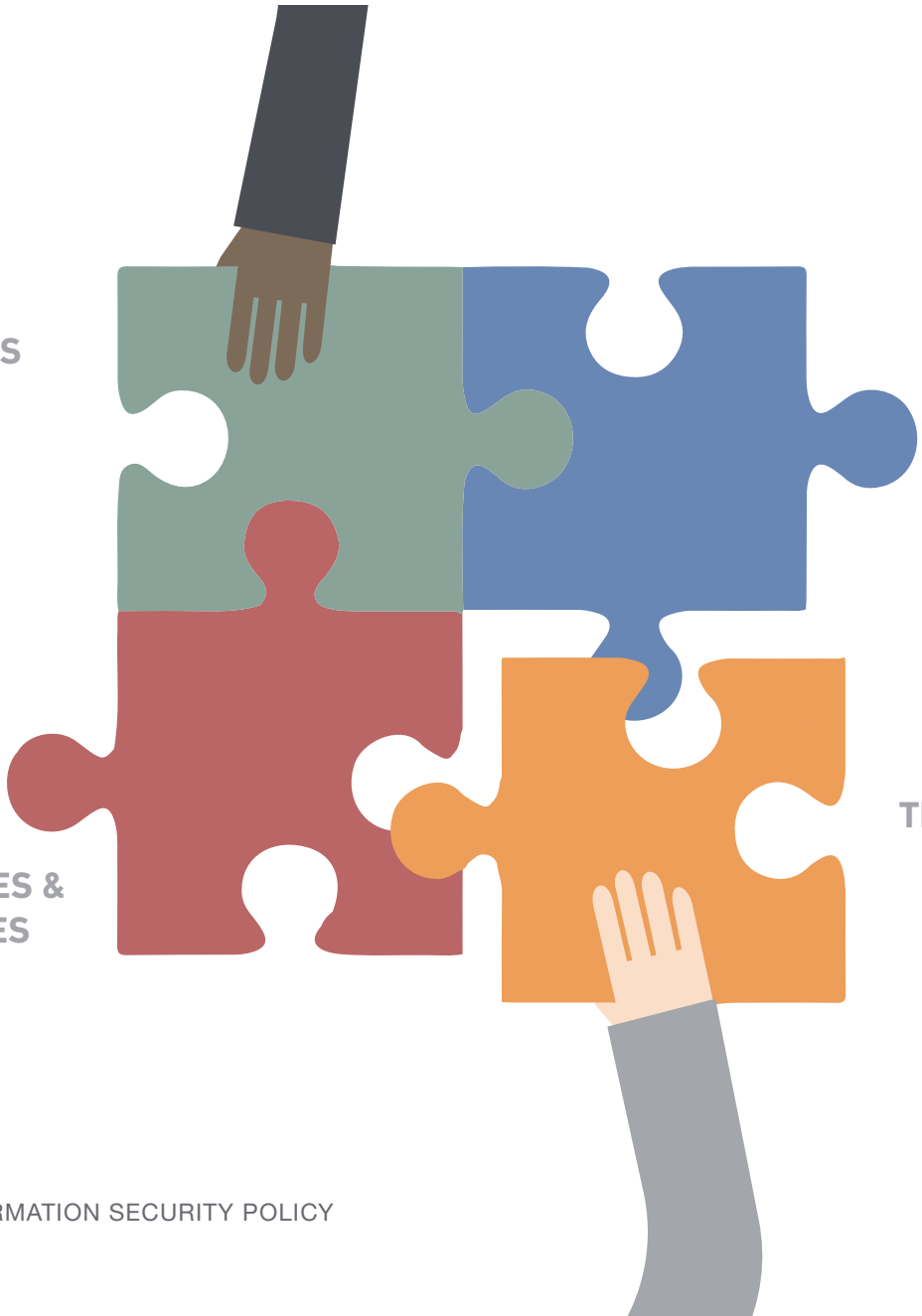
TECHNOLOGY

- 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.

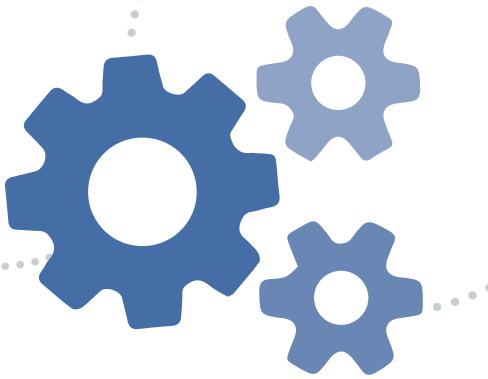
Through these enhanced and targeted awareness efforts, employee engagement and digital learning campaigns, and regular communications from the CISO and Information Security teams, we are nurturing a risk-aware culture across our organization and our resilience to social engineering continues to demonstrate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

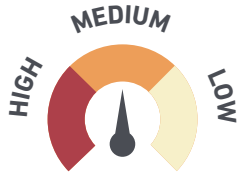
Analyzing Risks

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

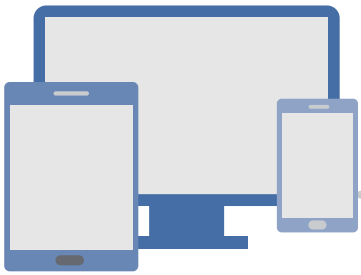
To safeguard our information assets, access is limited to authorized, business-justified entities with a "need to know." We have taken thorough measures to prevent the inappropriate use of access credentials:

- 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

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®