Segurança da Informação e Privacidade de Dados

Proteger e respeitar as Informações que nos são confiadas

Por que isso é importante

O mundo do trabalho está se tornando cada vez mais digital e orientado por dados, e a frequência e a sofisticação dos crimes cibernéticos estão aumentando. Nosso Centro de Excelência em Análise, Avaliação e Inovação de Pessoas é responsável por fornecer e pilotar novas inovações que geram impacto significativo para nossos negócios, incluindo avaliações, IA e aprendizado de máquina e nova tecnologia de plataforma. Como resultado, gerenciar nossa segurança da informação e saber como responder às preocupações éticas e de equidade da tecnologia emergente nunca foi tão vital.

Devemos articular nosso compromisso de sermos bons administradores das informações que nos são confiadas e assumir a responsabilidade de estar vigilantes e educar nosso povo com seriedade. Na cauda longa da COVID-19, a migração em massa para o trabalho remoto e a rápida digitalização dos processos exigem uma priorização ainda maior da segurança e privacidade da informação para proteger nossos dados e trabalhadores, garantindo confiança e transparência com nossos funcionários, clientes e parceiros.

Orgulhosos do nosso progresso: onde estamos hoje

Liderança no topo

Sob a direção do Chief Information Security and Chief Privacy Officer (CISO/CPO), a responsabilidade pelo nosso programa de segurança global reside nos mais altos níveis de liderança executiva, reportando-se ao Diretor Financeiro. O CISO/CPO reúne-se trimestralmente com o Comitê de Auditoria do Conselho de Administração para revisar e discutir a estratégia de segurança e o progresso em torno de nossos investimentos. Todos os membros da Equipe de Liderança Executiva estão incluídos em todos os treinamentos cibernéticos e campanhas de conscientização sobre phishing ao lado de toda a organização.

Além disso, para garantir que nossas inovações sejam construídas sobre nossa sólida base ética, contamos com nossa Força-Tarefa de IA Ética, liderada por nosso Diretor Jurídico, Diretor de Inovação e Diretor de Segurança da Informação,

para revisar e mapear inovações para as seguintes prioridades: privacidade de dados, segurança cibernética, supervisão humana, explicabilidade, robustez técnica e responsabilidade legal.

Padrões e Estruturas Globais

Nosso compromisso com os mais altos padrões de segurança da informação e privacidade de dados está descrito em nosso Código de Conduta e Ética de Negócios global. Disponível em 20 idiomas em nosso site corporativo, o Código é compartilhado com todos os funcionários e todas as partes interessadas em todo o mundo.

Nossa Política de Privacidade Global descreve os tipos de informações pessoais que coletamos de candidatos, associados e clientes, incluindo como as usamos, com quem as compartilhamos e os direitos e escolhas disponíveis para os indivíduos em relação ao uso de suas informações.

Mantidas em nível nacional, as políticas de privacidade dos funcionários (funcionários internos) estão alinhadas com nossos padrões globais e cumprem todas as leis e regulamentos locais. Um programa holístico de privacidade global foi estabelecido para garantir que os dados pessoais identificáveis de candidatos, associados, parceiros de negócios e funcionários sejam processados de forma a minimizar os riscos para os indivíduos.

Estabelecemos uma estrutura global abrangente de segurança da informação, alinhada com a norma ISO 27001 reconhecida internacionalmente, que todas as nossas operações em todo o mundo são obrigadas a adotar. Todos os data centers que suportam nossas principais operações de mercado (80% do nosso negócio) são certificados pela ISO 27001. Além disso, várias de nossas maiores operações no país (representando 39% das receitas mundiais) também mantêm a certificação ISO 27001 para seus sistemas locais de gerenciamento de segurança da informação.

Gerenciando riscos, protegendo indivíduos e organizações

Manter as informações seguras requer uma avaliação constante dos riscos. Nosso Programa Global de Risco e Segurança da Informação (GRIP) é uma estrutura de toda a organização que combina pessoas, processos e tecnologia para reduzir riscos, criar valor para nossos clientes e garantir que os dados que as pessoas nos confiam estejam protegidos.

Para garantir que estamos preparados para responder a incidentes e neutralizar efetivamente as ameaças, nossas equipes de InfoSecurity e Auditoria Interna trabalham com um terceiro independente para conduzir exercícios da Red Team que simulam ataques de segurança contra nosso ambiente anualmente. Nossos sistemas são continuamente testados quanto a vulnerabilidades por meio de testes de penetração adicionais e ferramentas e serviços de varredura automatizada.

Mantendo a segurança: treinando e mantendo a conscientização

A frequência e a sofisticação dos crimes cibernéticos estão aumentando, e levamos a sério nossa responsabilidade de estar vigilantes e educar nosso povo. Realizamos campanhas de conscientização continuamente, incluindo cursos de treinamento digital e exercícios de phishing por e-mail, além de exigir treinamento anual para todos os nossos funcionários sobre proteção de dados, privacidade e segurança da informação. É importante que também facilitemos para nossos funcionários relatar preocupações por meio da tecnologia de alarme de phishing integrada ao nosso sistema de e-mail, bem como nossa Política de Gerenciamento de Incidentes de Segurança da Informação, que descreve claramente o processo de comunicação e escalonamento para eventos relacionados à privacidade.

Atualizamos regularmente o treinamento para lidar com riscos emergentes ou mudanças nas regulamentações. Por exemplo, aprimoramos nosso treinamento em proteção de dados, privacidade e segurança cibernética em antecipação ao Regulamento Geral de
Proteção de Dados da União Europeia, à Lei de Privacidade do Consumidor da Califórnia e à Lei de Proteção de Dados Pessoais da Índia — educando e capacitando cada indivíduo a assumir a responsabilidade pela segurança e privacidade das informações.

Reportagem: Uma Linha Crítica de Defesa

Os funcionários desempenham um papel fundamental na identificação de possíveis problemas. Os funcionários são instruídos sobre como relatar atividades suspeitas em seu ambiente de trabalho ou a tecnologia que usam. A integração perfeita de segurança permite que a equipe denuncie e-mails suspeitos de phishing com um clique, e nossa Linha Direta de Ética Global está disponível a qualquer hora e de qualquer lugar, para que qualquer pessoa denuncie problemas ou busque orientação. Os problemas reportados por meio do disque-denúncia são reportados ao Comitê de Auditoria do Conselho de Administração.

Por meio de nossos esforços de conscientização aprimorados e direcionados, o engajamento dos funcionários, a resiliência à engenharia social e a conscientização geral continuam a demonstrar uma melhoria medida ano após ano.

Expandindo nossa equipe, aprofundando nossas capacidades

A centralização de nossa governança, operações e liderança de pensamento em segurança da informação e privacidade de dados levou a recursos de segurança e maturidade muito aprimorados em toda a empresa, permitindo a rápida implantação de recursos futuros. Nosso programa de segurança cibernética foi avaliado por um terceiro independente nos últimos três anos e mostrou capacidade medida e melhoria de maturidade ano após ano. Espera-se que esta tendência se mantenha no futuro próximo.

Nossa talentosa equipe dedicada à segurança da informação e privacidade de dados aumentou de tamanho significativamente nos últimos anos. Nosso pessoal está estrategicamente posicionado nos níveis de mercado global, regional e local para garantir a existência de políticas, processos e tecnologia consistentes em todos os locais, todos altamente treinados com certificações, incluindo CISSP, CISM, CISA, CRISC, CQA, Security+, CSCP, CIPM e CIPP/E.

Direitos e consentimento do titular dos dados

Os titulares dos dados e os consumidores são informados de forma transparente sobre como o ManpowerGroup gerencia seus dados e qual é a finalidade e os períodos de retenção de dados. A finalidade é claramente limitada e os períodos de retenção estão alinhados com os requisitos legais. Os titulares dos dados e os consumidores podem facilmente executar os seus direitos, incluindo o direito de aceder, retificar e eliminar os seus dados. Os mecanismos de consentimento e opt-out e opt-in são implementados de forma consistente e clara para permitir que os indivíduos tomem decisões informadas.

Cyber Safe em um local de trabalho híbrido

Nas fases iniciais da crise de saúde COVID-19, mudamos rapidamente para o trabalho remoto, mesmo antes dos lockdowns governamentais, a fim de garantir nossa prioridade PeopleFirst e a segurança de nossos funcionários, associados, clientes e comunidades. Mais de 80% de nossa equipe migrou para o trabalho remoto em um período de 10 dias, com a segurança dos dados mantida como prioridade.

Com mais de 20.000 funcionários usando novas tecnologias em novos locais, reconhecemos a necessidade de ajudar nosso pessoal a exercer ainda mais vigilância e criamos o Cyber Safe at Home, uma série de capacitação para aumentar nossa consciência cibernética enquanto trabalhamos em casa. O programa incluiu orientações sobre o uso seguro e eficaz de ferramentas de colaboração (nossas e de outros), ficar atento a ataques de phishing, dicas de segurança exclusivas para COVID-19 e bons hábitos de segurança online para uso no trabalho e em casa.

Com uma força de trabalho híbrida agora em vigor, continuamos a fornecer orientação contínua sobre o Cyber Safe at Home.

Reconhecimento Externo

Em reconhecimento às nossas abordagens de segurança cibernética, fomos reconhecidos como vencedores do prêmio CS050. Os prêmios CSO50 reconhecem projetos de segurança que demonstram liderança de pensamento excepcional e valor comercial.