



Cybersecurity Governance

At PSRH Global, maintaining the trust of our clients, candidates, and employees is one of our top priorities. We achieve this by effectively managing the risks associated with the security, confidentiality, and integrity of the data we collect. To this end, we have implemented comprehensive security measures across organizational, architectural, and operational levels to ensure our data remains protected.

Security Governance

Our cybersecurity initiatives are overseen by senior leadership, with the Chief Information Security Officer (CISO) at the helm. The CISO is responsible for defining and guiding our data and information security strategy, ensuring that the company is well-prepared to address cybersecurity risks. Updates regarding cybersecurity efforts and actions to mitigate risks are regularly provided to the Board of Directors.

Information Security Management System

Introduction

PSRH Global is dedicated to protecting its data and assets from both internal and external threats. Our approach to information security focuses on prevention, detection, and response, informed by threat intelligence, risk assessments, and proactive monitoring. Our goal is to safeguard not only the company's systems and data but also the information of our clients, candidates, and employees.

Risk Governance

Risk management is embedded in PSRH Global's culture and business practices. We conduct ongoing risk assessments to identify, monitor, and analyze risks, ensuring that we address any emerging issues promptly.

Risk Governance Framework

We follow a **three-line defense model** that organizes risk management across our business units, independent oversight functions, and internal audit, promoting accountability and comprehensive risk oversight.

Information Security Oversight

Information security is managed by our Chief Information Security Officer (CISO), who reports directly to senior leadership. The CISO ensures that the company is aligned with best practices and regulatory requirements and provides regular updates on security efforts, program status, and incidents.



Technology Risk Management

The CISO oversees technology risk management, which includes conducting regular security assessments in several key areas:

1. Core business processes and information assets
2. Internet-facing services
3. Technology project development lifecycle
4. Supplier security due diligence
5. Vulnerability assessments based on threat intelligence

Internal Audit

Our internal audit team evaluates the company's overall control environment and reports to the audit committee of the Board of Directors. This ensures the effectiveness of our governance, risk management, and security controls.

Industry Engagement

PSRH Global is an active participant in industry initiatives focused on advancing data security and privacy standards.

Information Security Policies and Standards

PSRH Global has established a comprehensive set of information security policies and standards to guide our approach to safeguarding data. These policies are regularly reviewed and approved by relevant governance bodies. Our information security standards align with industry best practices and regulatory requirements, covering areas such as identity and access management, software security, mobile security, and data protection.

Training and Education

We offer a security awareness program to help employees recognize and respond to cybersecurity threats. Employees are required to complete annual information security training, which covers topics such as cybersecurity essentials, data risk management, and phishing awareness.

Identity and Access Management

PSRH Global has implemented strong controls to authenticate and authorize access to systems and information assets, including multi-factor authentication.

Access Management



We adhere to strict access management protocols, ensuring that only authorized individuals can access company resources. Access rights are reviewed regularly, especially when employees change roles, and restrictions are applied based on regulatory, security, and internal control requirements.

Application and Software Security

We manage application and software security through regular assessments, security testing, and proactive logging capabilities.

Security Testing

We conduct penetration tests to evaluate the security of our infrastructure and identify potential vulnerabilities. These tests are based on industry-standard guidelines to ensure thorough evaluation.

Data Backup and Recovery

All critical data is encrypted and securely backed up to enable recovery if necessary, using industry-standard systems and practices.

Infrastructure Security

PSRH Global protects its infrastructure through a layered network architecture, regular vulnerability assessments, system hardening, and malware protection.

System Monitoring and Vulnerability Management

We have a comprehensive vulnerability management program that includes regular vulnerability scans of both internal and external systems. Third-party providers also conduct external scans to identify security weaknesses.

Cloud Infrastructure

We conduct thorough security reviews of cloud service providers to ensure that they meet our security standards and regulatory requirements.

Mobile Security

PSRH Global provides secure mobile access solutions to protect company data on mobile devices, incorporating encryption and multi-factor authentication.

Mobile Security



Company-approved mobile applications use industry-standard security controls to protect both internal systems and client interactions.

Data Security

PSRH Global applies strong data security controls to protect sensitive information, both during transmission and at rest.

We have established clear desk policies to ensure sensitive data is securely stored and disposed of. Employees are trained to protect confidential information, and secure data disposal methods such as shredding are in place.

Physical Security

PSRH Global implements robust physical security measures at its facilities, including secure access controls, video surveillance, and environmental safeguards to protect our data and assets.

Our data centers are equipped with advanced physical security measures, including redundant power supplies, fire suppression systems, and environmental protections to ensure the continuity of service in the event of a disruption.

Supplier Security

We integrate information security into our supplier management process, ensuring that all suppliers adhere to our security standards.

Supplier Security

Suppliers who handle sensitive data are required to undergo security assessments based on the type and volume of data they process. These assessments help us evaluate the effectiveness of their information security and privacy practices.

Security Incident Management

PSRH Global has a comprehensive incident management program to address potential security threats that could impact the confidentiality, integrity, or availability of our data.

Incident Management

Our incident management team is responsible for identifying, responding to, and escalating security incidents as needed. We have a Cybersecurity Incident Response Plan that outlines procedures for addressing incidents, including client notification and legal compliance in the event of a breach.



Business Continuity and Disaster Recovery

We have established programs to ensure business continuity, disaster recovery, and technology resilience, ensuring that we are prepared to respond to any disruptions effectively.

Business Continuity

Each business unit has a dedicated Business Continuity Plan (BCP) that is regularly updated and tested to ensure preparedness in the event of an emergency.

Crisis Management and Emergency Response

Our crisis management team monitors potential threats and implements pre-established procedures to manage crises, ensuring a coordinated and effective response during emergencies.

Protecting Yourself from Recruitment Scams

Recently, we've noticed a concerning rise in recruitment scams, where fraudsters impersonate legitimate recruitment companies or consultants to deceive individuals. At **PSRH Global**, we are committed to raising awareness about these fraudulent tactics to help protect both candidates and organizations from scammers using our name or the names of our consultants.

Warning Signs to Look Out For

To help you stay vigilant, we've compiled a list of warning signs that may indicate you've been contacted by a scammer posing as a recruitment consultant or company:

Requests for Personal Financial Information

- A recruiter or company requesting personal financial details.
- A request for payment to be considered for a role or to secure an interview.
- A request for money on behalf of another individual.

Suspicious Social Media Activity

- The purported recruiter's profile on platforms like LinkedIn, WhatsApp, or Telegram lacks activity, information, or contact details.
- No profile picture or a suspiciously generic one.
- Communications that seem unprofessional or too informal, such as contact made through WhatsApp or Telegram without a valid reason.

Guarantees of Employment or Income



- Be wary of anyone guaranteeing employment or income upfront. **PSRH Global** will never request any form of direct payment from candidates, nor will we contact you via WhatsApp, Telegram, or similar apps.

At **PSRH Global**, our priority is to create a secure and transparent recruitment process. If you ever feel unsure about any communication you receive, please reach out to us directly to verify its legitimacy.