HEIDRICK & STRUGGLES

CORPORATE INFORMATION SECURITY MEASURES

INTRODUCTION

This document describes the information security requirements and measures used to establish and enforce the corporate information security program at Heidrick & Struggles International, Inc., and its affiliates ("Heidrick & Struggles").

Protecting data and the systems that collect, process, and maintain this information is of utmost importance. The security of Heidrick & Struggles' systems comprises controls and safeguards to mitigate risks, potential threats, and ensure accountability, availability, integrity, and confidentiality of the data.

SCOPE AND APPLICABILITY

The Information Security requirements and measures described in this document apply to Heidrick & Struggles' internal security with respect to our systems, applications, and networks.

1. INFORMATION SECURITY PROGRAM

Heidrick & Struggles defines information security roles and responsibilities within its organization. Led by the Heidrick & Struggles' Chief Information Security Officer ("CISO"), the Heidrick & Struggles' Information Security team is responsible for securing its systems, applications, and networks.

Heidrick & Struggles' corporate information security program aligns with the ISO 27001 and NIST SP 800-53 frameworks.

2. INFORMATION SECURITY POLICIES

Heidrick & Struggles maintains a written information security policy supplemented by additional internal standards, procedures, and guidelines that defines employees' responsibilities with respect to Heidrick & Struggles' corporate information security program. These policies and procedures are (i) evaluated and updated regularly, and (ii) made available to all Heidrick & Struggles personnel.

3. INFORMATION SECURITY AWARENESS AND TRAINING

All Heidrick & Struggles personnel (employees and contractors) undergo security awareness training during the initial onboarding process and then on an annual basis thereafter. Additionally, security awareness campaigns are conducted regularly and include simulated social engineering tactics.

4. PERSONNEL SECURITY

Heidrick & Struggles engages a reputable, commercially recognized background check or investigative entity to conduct background checks, as permitted by applicable law, on all new hires. Background checks may include criminal history checks, education verifications, employment verifications, and credit checks.

Additionally,

  - Heidrick & Struggles requires that all personnel enter into written confidentiality agreements.
  - Heidrick & Struggles has a disciplinary process in place for policy violations.
- Heidrick & Struggles promptly terminates access to Heidrick & Struggles' systems, applications, and networks when personnel depart from Heidrick & Struggles.

5. THIRD-PARTY RISK MANAGEMENT

Under Heidrick & Struggles' Third-Party Risk Management (TPRM) program, all third-parties' security controls are comprehensively assessed at the onset of the relationship and on an ongoing basis thereafter. This assessment includes reviews of their security and data protection documentation e.g., SOC2 audit reports and security certifications like ISO 27001, as well as responses to Heidrick & Struggles robust Third-Party Due-Diligence questionnaire. In some cases, an on-site audit is conducted.

Heidrick & Struggles ensures appropriate contractual agreements are in place before engaging third-party providers; these include Security, Privacy and Confidentiality agreements that meet or exceed our requirements.

6. OFFICES

Heidrick & Struggles' offices are located in professionally managed buildings with controlled entry points, 24 x 7 on-site security, and CCTV.

Access to Heidrick & Struggles offices is restricted to appropriate personnel, granted in accordance with the principle of least privilege and subject to security monitoring. Personnel and visitors are expected to wear clearly visible badges at all times while on company property.

7. DATA CENTERS

Heidrick & Struggles data centers are Tier III and above, ensuring extensive security controls including secure design, access control, logging and monitoring, surveillance and detection, device management, and infrastructure maintenance.

8. NETWORK SECURITY

Heidrick & Struggles deploys firewalls to secure the perimeter of its network segments. By employing a Zero-Trust Network Architecture (ZTNA), network traffic must pass through firewalls, secure web gateways, and encrypted tunnels that are constantly monitored.

The components of Heidrick & Struggles ZTNA implementation include intrusion prevention systems (IPS) to detect and prevent potential network compromises. Network security controls are assessed on a regular basis by reputable third-parties that perform internal and external penetration tests.

9. ACCESS CONTROL

Heidrick & Struggles implements and maintains rigorous access controls mechanisms intended to prevent unauthorized access, limiting access to authorized users in accordance with the principle of least privilege.

- Heidrick & Struggles uses role-based access control ("RBAC") to ensure personnel only have access commensurate to their job function.
- Heidrick & Struggles requires strong password control parameters (i.e., length, character complexity, and non-repeatability).
- Heidrick & Struggles requires secure Multi-Factor Authentication (MFA) which require combinations of device-trust certificates, authenticator apps, risk-based conditional access policies, etc.
- Heidrick & Struggles does not permit the use of shared accounts.
- Heidrick & Struggles leverages an access management program for provisioning (i.e., assigning, modifying, or revoking) user access for all systems and applications.

- Heidrick & Struggles revokes access to its information systems promptly after an individual ceases employment with the company.

10. ENDPOINT DEVICES

Heidrick & Struggles' personnel are required to use managed endpoint devices configured with appropriate security controls and in accordance with the applicable configuration baseline.

Endpoint devices must (i) be configured for automatic patching; (ii) be encrypted (i.e., full disk, endpoint encryption); (iii) be secured with a protected (password) screen lock with the automatic activation feature; (iv.) be periodically scanned for restricted/prohibited software; (v.) not be rooted or jailbroken; and (vi.) run an acceptable industry standard antimalware solution for which on-access scan and automatic update functionality is enabled.

Mobile devices must be enrolled in Heidrick & Struggles' Mobile Device Management ("MDM") program to access corporate application. Heidrick & Struggles' MDM program enforces security requirements, including remote wiping capability and OS version updates.

11. APPLICATION SECURITY

Heidrick & Struggles has a formal and documented Secure Software Development Lifecycle (S-SDLC) that is reviewed at least annually, and integrates security best practices during each phase of the SDLC.

Developed applications are thoroughly tested for vulnerabilities prior to deployment. Heidrick & Struggles segregates environments for development, testing, and production, and uses commensurate security measures to secure each environment based on data classification.

All developed applications, components, and underlying infrastructure are regularly audited, including penetration testing by an external third-party.

Application and software development processes are integrated in the organizational security risk and change management processes.

12. ASSET MANAGEMENT

Heidrick & Struggles maintains an inventory of assets. Heidrick & Struggles' decommissioning and destruction policy outlines the requirements for secure asset and data destruction

13. CHANGE MANAGEMENT

Heidrick & Struggles' Change Advisory Board ("CAB") evaluates all changes to systems, applications, services, and capabilities prior to deployment in Heidrick & Struggles' production environments.

Heidrick & Struggles separates development and production environments to reduce the risks of unauthorized access and/or changes to the operational system or information.

14. VULNERABILITY MANAGEMENT

Heidrick & Struggles performs internal and external network vulnerability scans on a regular basis. Identified vulnerabilities are remediated and/or mitigated in a timely manner, according to the severity and risk exposure.

15. LOGGING

Audit logging is enabled on Heidrick & Struggles' corporate systems and applications; these audit logs are configured to capture sufficient detail (i.e., timestamp, event status, user details, etc.,). Where feasible, all logs are aggregated and centralized via Heidrick & Struggles' SIEM platform where they are immutably retained for one (1) year. A dedicated security operations team monitors logs for indicators of compromise, suspicious or malicious activity.

16. INCIDENT RESPONSE

Heidrick & Struggles maintains a management-approved, detailed incident response plan that is activated whenever Heidrick & Struggles becomes aware of a suspected data breach or security incident. The Incident Response plan include procedures to identify, report and appropriately respond to security incidents and/or data breaches.

Heidrick & Struggles promptly notifies impacted individuals or client organizations of a security incident. Heidrick & Struggles provides accurate information and reasonably cooperates with clients to fulfill data breach reporting obligations under applicable laws.

17. BUSINESS CONTINUITY AND DISASTER RECOVERY

Heidrick & Struggles maintains a Business Continuity Management program to limit business disruption, prevent data loss, and ensure timely restoration in the event of system failure, damage, or destruction. Business continuity and disaster recovery ("BC/DR") plans are established for all business-critical assets or systems and are reviewed and tested at least annually.