HEIDRICK & STRUGGLES INTERNATIONAL, INC.

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," "the company").

Protecting data and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of Heidrick & Struggles' systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data.

Scope and applicability

The measures described in this document apply to Heidrick & Struggles' security with respect to our network infrastructure, applications, and other Information systems.

SECURITY MANAGEMENT

1. Information Security program

Heidrick & Struggles defines information security roles and responsibilities within its organization. Heidrick & Struggles' Chief Information Security Officer ("CISO") oversees the program.
Heidrick & Struggles has a dedicated Information Security team responsible for the security of its network, applications, and systems. Heidrick & Struggles' information security program is aligned with the ISO 27001:2013 and NIST SP 800-53 r5 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 evaluated and updated regularly and made available to all Heidrick & Struggles personnel.

3. Security awareness and training

All Heidrick & Struggles personnel (employees and contractors) undergo security awareness training during the initial onboarding process and on an annual basis thereafter.

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, education & employment verifications, and credit checks.

Heidrick & Struggles ensures that all personnel enter into written non-disclosure/confidentiality agreements.

Heidrick & Struggles has a disciplinary process in place for policy violations.

Heidrick & Struggles promptly terminates personnel access to Heidrick & Struggles' information systems when an individual separates or discontinues work for Heidrick & Struggles.

5. Vendor risk management

Heidrick & Struggles has a third-party risk management (TPRM) process where, at the onset of a relationship, the third party's security controls are comprehensively reviewed and then on a regular basis. As part of the TPRM, vendors participate in security assessments, which include reviews of their security documentation or certifications, e.g., SOC1/SOC2. In some cases, an onsite audit is performed.

Heidrick & Struggles ensures appropriate security clauses are added to service agreements. Heidrick & Struggles' Procurement and Legal teams review proposed vendor engagements. For those vendors that will have access to Heidrick & Struggles' internal networks and/or will store, process, or transmit data, Heidrick & Struggles assesses the security and privacy practices of such vendors to ensure they meet a standard that is appropriate to the data classification and scope of services they are engaged to deliver. Vendors are required to agree to appropriate security, confidentiality, and privacy contract terms with Heidrick & Struggles based on the risks presented by the vendor risk assessment.

When engaging third-party providers of products and services, Heidrick & Struggles requires non-disclosure agreements be in place with any potential vendor before engaging in discussions regarding a potential business arrangement.

PHYSICAL SECURITY

6. Office security

Heidrick & Struggles' facilities team is responsible for implementing physical and environmental security controls for office locations in accordance with Heidrick & Struggles' Physical Security Policy. Access to Heidrick & Struggles offices is restricted to appropriate personnel and granted in accordance with the principle of least privilege and subject to monitoring measures. Employees, vendors, contractors, and visitors are always expected to wear their badges in a clearly visible fashion while on company property.

Our offices are in professionally managed buildings with card access systems, receptionists, 24/7/365 on-site security, and CCTV.

7. Datacenter security

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

SYSTEMS SECURITY

8. Network security

Heidrick & Struggles deploys firewalls to achieve perimeter protection as well as internal network segmentation of Heidrick & Struggles' networks. By design, all network traffic must pass through firewalls, which are always monitored.

Heidrick & Struggles has implemented and maintains an intrusion prevention system to detect and stop potential network compromises.

Heidrick & Struggles engages a reputable third-party firm to perform regular internal and external penetration tests on its network.

9. Access control

Heidrick & Struggles has implemented and maintains access control mechanisms intended to prevent unauthorized access and limit access to users who have a business need to know in accordance with the principle of least privilege.

Heidrick & Struggles personnel must comply with Heidrick & Struggles' internal Acceptable Use Policy.

Heidrick & Struggles leverages an access management program for provisioning, modifying, and de-provisioning user access to all systems and applications. All access requests are approved by management prior to permissions being granted. Access permissions are reviewed at least quarterly.

Heidrick & Struggles uses role-based access control ("RBAC") to ensure personnel only have access commensurate to their job function. The use of shared user accounts is not permitted.

Heidrick & Struggles requires strong password control parameters (i.e., length, character complexity, and non-repeatability).

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

Access to Heidrick & Struggles corporate applications requires multi-factor authentication via Heidrick & Struggles' SSO platform.

Remote network access requires multi-factor authentication and must employ Heidrick & Struggles' VPN solution.

10. Endpoint security

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

Endpoint devices must, at a minimum,

a) have a supported operating system
b) be encrypted with full disk symmetric encryption
c) run an approved anti-malware solution with automatic updates
d) be secured with a password-protected automatic screen lock after a period of inactivity
e) be kept up to date with the latest security patches
f) be periodically scanned for restricted/prohibited software
g) not be rooted or jailbroken

Mobile devices must be enrolled in Heidrick & Struggles' Mobile Device Management (MDM) in order to access Heidrick & Struggles' corporate applications. Heidrick & Struggles' MDM enforces the security requirements and provides capabilities, including remote wiping and OS version updates.

11. Application security

Heidrick & Struggles has a formal and documented Secure Software Development Lifecycle that is reviewed at least annually.

Heidrick and Struggles integrates security best practices during each phase of the SDLC.

Developed applications are thoroughly tested for vulnerabilities prior to deployment.

Heidrick & Struggles has segmented 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 tests by an external party.

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

COMPLIANCE

12. Asset management

Heidrick & Struggles maintains an up-to-date inventory of assets

Heidrick & Struggles has a formal policy on asset decommissioning and destruction. The policy outlines the requirements for assets and data to be securely destroyed.

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 runs 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 they pose to our systems.

15. Logging

Audit logging is enabled on Heidrick & Struggles' systems and applications; such audit logs are configured to capture sufficient detail and are centralized in a SIEM where it is correlated and reviewed for anomalies by the dedicated security team.

16. Incident Response

Heidrick & Struggles maintains an incident response program to identify, report, and appropriately respond to known or suspected security incidents and/or personal data breaches.

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.

Heidrick & Struggles will notify any impacted individuals or client organizations of a security incident in a timely manner. Heidrick & Struggles will provide accurate information and reasonable cooperation for a client to fulfill its data breach reporting obligations under applicable laws.

Heidrick & Struggles will take measures and actions as it considers necessary to remedy or mitigate the effects of a security incident or personal data breach.

BUSINESS CONTINUITY AND DISASTER RECOVERY

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

Adopted: October 2023