Information Security: 39 Questions to Ask Your Screening Provider

The following questionnaire is a sample guide for organizations seeking to assess overall information security risks related to background screening providers. This document was created as a model only and additional questions should be considered based on the size, scope and relationship with the potential screening provider.

Information Security Policy and Objectives

1. Does your company maintain a documented information security policy and objectives?
   a. If so, how is it managed and who is authorized to update it?
   b. How often are the policy and objectives updated?
   c. How is training conducted for awareness?
   d. Are there disciplinary actions for non-compliance?

Physical Security

2. Describe the security features used to protect your operational facility.
   a. Your overall access control policy
   b. Do you utilize security badges?
   c. Do you use surveillance or other devices to monitor employees and visitors?
   d. How do you track visitors and contractors?

Processing, Storage and Transfer of Personally Identifiable Information (PII)

3. Does your company have documented procedures in regard to the processing, storage and transfer of PII?
4. How do you define PII within your organization?
5. What are the minimum confidentiality requirements around processing, storage and transfer of PII?
6. How is training conducted around proper use of PII?
7. What happens if PII is mishandled or transferred to an authorized party?
8. What are the disciplinary actions for mishandling PII?
9. Are there audits conducted around proper handling of PII?

Human Resource Security

10. Are confidentiality agreements maintained for all contractors and employees? If yes, what are the primary areas addressed within the agreements?
11. What are the specific types of background checks used to assess candidates for employment?
    a. Are they conducted on a pre-employment basis?
    b. What about ongoing background checks?
    c. Are employees required to self-report any criminal activity that may affect their employment with the company?
12. How are employees trained around information security risks?
    a. What areas are addressed within training?
    b. How is ongoing training addressed?
    c. Are there disciplinary actions for non-compliance?

Internal Audit Controls

13. Do you conduct internal audits regarding information security?
    a. What types of internal audits are conducted and by whom?
    b. Are audits scheduled and documented?
    c. What oversight exists for audit results?
    d. How are non-conformance with policies and procedures addressed?

Change Management

14. How is change managed throughout the organization in regards to information and information assets?
    a. Do you maintain a documented change management procedure?
    b. How is change monitored and controlled?
    c. How is information security managed through projects?

Information Asset Management

15. Are different types of information classified within your organization? If yes, what are the classifications?
16. How do you protect leakage of confidential client information?
17. How is client data stored both physically and logically?
18. What is the communication protocol to clients when confidential information is compromised?

Managing Third-Party or Outsourced Partnerships

19. Do you have documented procedures for vetting and ongoing assessment of third parties handling client information?
    a. What vetting requirements are used to assess third parties before handling client data?
    b. What types of agreements are in place to protect client data with third parties?
    c. What types of audits are conducted on third parties with access to client data?
    d. Are there notification requirements in place if client data is misdirected?

Business Continuity

20. Does your organization have a business continuity or business resumption plan?
    a. If yes, what are the key areas addressed within the plan?
    b. How are information backups managed throughout the organization and how is the restoration of data tested?
    c. How often is the plan tested and under what conditions?
    d. What Service Level Agreement (SLA) can you provide regarding operational up time?
    e. How are events that may affect operations communicated to clients?

Use of Datacenters

21. Do you utilize an outsourced or offsite datacenter as part of your operations?
    a. If yes, what are the data security attributes of the center?
    b. Do you have an SLA with your datacenter? If yes, what are the details?
    c. Does the datacenter carry any type of information security certifications?

Management’s Role in Information Security

22. Who is in charge of information security at your organization?
23. How does management play a role in information security?
24. How are information security policies communicated through management?

Information Lifecycle Management

25. Describe the process for following information throughout its lifecycle in your organization.
    a. Do you use information classifications? If yes, describe what types?
    b. Who has access to PII?
    c. What happens to electronic and hardcopy information that is no longer needed?

Security Incident Management

26. Does your organization have a documented procedure for incident management?

27. How do you train staff around information security events?
28. Do you have a management team that deals with such events? Does the team practice incident scenarios?
29. What is the communication protocol around reporting events to clients?
30. What is the procedure to deal with PII that has been misdirected?
31. Have you ever experienced a security breach within your organization? If yes, provide details?

Access Control

32. Does your organization have an access control policy? If yes, describe the policy at a high level in regards to the type of network access.
    a. How do you manage network access for staff and internal contractors?
    b. How do you manage access control for clients?
    c. Do you audit access control? If yes, how often and to what length?

Encryption

33. Describe your use of encryption when accessing information networks or accessing systems through public networks.
    a. What is the minimum encryption protocol used to access PII?
    b. What type of encryption is used to transfer data between third-party suppliers?
    c. What type of encryption is used for client access to data?

Password

34. Describe your password control policy.
    a. What is the minimum complexity requirement for network passwords?
    b. How often are network passwords changed? Are they required and is the process automated?
    c. Describe the process for managing client passwords.

Compliance

35. Describe your company's efforts around statutory and regulatory compliance.
    a. Do you have a compliance department or a dedicated person focused around compliance?
    b. If yes, how is compliance monitored to keep up with industry trends?
36. How are compliance changes communicated with internal staff and clients?
37. Do you conduct compliance audits? If yes, how often and who conducts the audits?

Software Development

38. How is software development handled within your organization?
    a. If outsourced, what are the oversight measures put in place to address information security in system development?
    b. Describe the processes for pushing out new software releases to clients
    c. Do you utilize a testing environment before deployment?
    d. How are software changes communicated to clients?

Information Security Certifications

39. Describe any information security certifications held by your organization or by members of your organization.