Security Operating Procedure

|  |  |
| --- | --- |
| **Procedure Name** | Vendor Monitoring & Review |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Approved By | Owner | Date Last Updated | Review Frequency | Next Review | Comments |
|  |  |  |  |  |  |  |

**Classification**: Confidential

This document should be restricted to those with a specific need.

**1. Purpose**  
This procedure establishes guidelines for the ongoing monitoring and review of third-party vendors to ensure compliance with contractual security requirements and to protect [Your Organisation's Name] from potential security risks.

**2. Scope**  
This procedure applies to all third-party vendors that provide goods or services to [Your Organisation's Name], especially those with access to sensitive data or critical systems.

**3. Roles and Responsibilities**

* **Vendor Management Team:** Responsible for coordinating and conducting vendor monitoring and reviews.
* **IT Security Team:** Assists in evaluating the security posture of vendors during the monitoring process.
* **Information Security Manager:** Reviews vendor compliance reports and ensures alignment with security policies.
* **Procurement Team:** Ensures that vendors meet ongoing contractual security requirements.

**4. Procedure**

**Step 1: Initial Setup**

* **Vendor Inventory:**
  + Maintain an up-to-date inventory of all third-party vendors, including details about the services they provide and their access level to sensitive data.
* **Risk Categorisation:**
  + Categorise vendors based on their risk level (e.g., low, medium, high) considering data sensitivity, access level, and the services' criticality.

**Step 2: Monitoring Schedule**

* **Regular Monitoring:**
  + Establish a schedule for regular monitoring of vendors based on their risk categorisation. High-risk vendors may require more frequent monitoring than low-risk vendors.
* **Continuous Monitoring:**
  + Implement continuous monitoring tools to track vendor activities, especially those interacting with critical systems or sensitive data.

**Step 3: Monitoring Activities**

* **Compliance Checks:**
  + Regularly review vendor compliance with contractual security requirements, including data protection measures, incident response protocols, and regulatory obligations.
* **Security Assessments:**
  + Conduct periodic security assessments, such as vulnerability scans, penetration testing, and security audits, to evaluate the vendor's security posture.
* **Performance Metrics:**
  + Monitor vendor performance against defined security metrics and key performance indicators (KPIs).

**Step 4: Review Process**

* **Documentation Review:**
  + Review the vendor's security policies, procedures, and relevant documentation to ensure they meet the agreed-upon standards.
* **Audit Reports:**
  + Analyse audit reports and findings from security assessments to identify potential risks and areas for improvement.
* **Incident Reports:**
  + Review any security incidents reported by the vendor and assess their response and remediation efforts.

**Step 5: Risk Mitigation**

* **Action Plans:**
  + Develop action plans to address any identified risks or non-compliance issues. Work with the vendor to implement necessary improvements.
* **Follow-Up Reviews:**
  + Schedule follow-up reviews to ensure the vendor has addressed identified issues and complies with security requirements.
* **Escalation:**
  + Escalate unresolved issues to senior management and consider renegotiating or terminating the contract if the vendor fails to meet security requirements.

**Step 6: Reporting and Documentation**

* **Compliance Reports:**
  + Prepare regular reports on vendor compliance and security performance, highlighting any issues and mitigation efforts.
* **Record Keeping:**
  + Maintain detailed records of all monitoring activities, assessments, and reviews in a central repository for future reference and audit purposes.
* **Stakeholder Communication:**
  + Communicate the results of vendor monitoring and reviews to relevant stakeholders, including the Vendor Management Team, IT Security Team, and senior management.

**5. Security Controls**

* **Access Control:** Ensure that vendor monitoring tools and documentation access is restricted to authorised personnel only.
* **Logging:** Maintain detailed logs of all monitoring activities, assessments, and reviews.
* **Review and Auditing:** Regularly review and audit the vendor monitoring and review process to ensure compliance with policies and identify areas for improvement.

**6. Incident Management**

* **Incident Identification:** Monitor for any incidents involving third-party vendors.
* **Incident Response:** Report and respond to incidents promptly, ensuring they are investigated and resolved.
* **Incident Documentation:** Document all incidents and the actions taken in response.

**7. Continuous Improvement**

* **Post-Review Analysis:**
  + Conduct post-review analysis to identify lessons learned and improve the vendor monitoring and review process.
* **Training:**
  + Provide ongoing training to relevant personnel on vendor monitoring and review practices.

**8. Review and Update**

* **Review Frequency:**
  + This procedure will be reviewed annually.
* **Update Process:**
  + The Information Security Manager must approve any updates or changes to this procedure.

**9. References**

* **Information Security Policy**
* **Vendor Management Policy**
* **Vendor Risk Assessment Report Template**
* **Regulatory Compliance Guidelines**