Third-Party Risk Management (TPRM) Policy Template for Premier Technology Solutions

**1. Purpose**

To establish a structured framework for identifying, assessing, and mitigating risks associated with third-party vendors, ensuring compliance with regulatory requirements and safeguarding Premier Technology Solutions’ data, systems, and reputation.

**2. Scope**

Applies to all third parties that:

* Access Premier’s Microsoft Azure cloud environment, Salesforce CRM, or internal systems.
* Process personally identifiable information (PII) or financial data (e.g., payroll providers).
* Provide critical services (e.g., AWS for cloud hosting, ADP for payroll).

**3. Vendor Risk Tiers**

Premier classifies vendors into three tiers based on data sensitivity and business impact:

|  |  |  |
| --- | --- | --- |
| **Tier** | **Criteria** | **Premier-Specific Examples** |
| High | - Direct access to **Azure-hosted client databases** or **PCI DSS-regulated payment systems**. | AWS, Microsoft 365, *Xero* (payroll). |
| - Critical to 24/7 SOC operations (e.g., *Splunk SIEM providers*). |  |
| Medium | - Access to internal tools (e.g., *Jira*, *ServiceNow*). | HubSpot, *Atlassian*, IT support vendors. |
| - Moderate impact if compromised (e.g., marketing analytics platforms). |  |
| Low | - No access to sensitive systems (e.g., office supply vendors). | Officeworks, janitorial services. |

**4. Vendor Onboarding Process**

1. **Risk Assessment**:
   * Complete Premier’s Vendor Risk Assessment Questionnaire, including:
     + Data encryption practices (e.g., AES-256 for data at rest).
     + Compliance certifications (e.g., ISO 27001, SOC 2).
   * Submit evidence of Essential Eight Maturity Level 2 compliance for high-risk vendors.
2. **Due Diligence**:
   * Financial health check via *Dun & Bradstreet*.
   * Review of past incidents (e.g., ransomware attacks, data breaches).
3. **Contractual Requirements**:
   * Include Premier’s Standard Data Processing Addendum (DPA).
   * Mandate breach notification within 12 hours (vs. industry-standard 72 hours).
4. **Approval**:
   * **High-risk vendors**: Require sign-off by CISO (John Doe) and Legal Counsel (Jane Smith).

**5. Contractual Clauses**

All contracts must include:

* **Breach Notification**: Vendors must notify Premier’s SOC ([**testsoc@premiertech.com**](mailto:testsoc@premiertech.com)) within 12 hours of detecting an incident.
* Data Sovereignty: Data must reside in Australian data centers unless explicitly approved.
* **Penetration Testing**: Vendors must allow Premier to conduct annual pen tests on their systems.
* **Subcontractor Oversight**: Vendors must disclose subcontractors (e.g., AWS sub-processors) for Premier approval.
* **Termination**: Immediate termination if vendors fail two consecutive audits.

**6. Contractual Clauses**

|  |  |  |
| --- | --- | --- |
| **Tier** | **Audit Frequency** | **Audit Requirements** |
| High | Biannual | - Third-party ISO 27001 audit. |
| - Premier-led vulnerability scan using *Qualys*. |
| Medium | Annual | - Internal audit of access logs. |
| - Review of patch management compliance. |
| Low | Ad-hoc | - Spot-check during contract renewal. |

**7. Ongoing Monitoring**

* **Continuous Risk Scoring**:
  + Use *SecurityScorecard* to monitor vendors’ security ratings.
  + Integrate alerts into Premier’s *Splunk SIEM* for real-time visibility.
* **Quarterly Reviews**:
  + High-risk vendors: Validate compliance with **ACSC Essential Eight** (e.g., application whitelisting, patching).
  + Medium-risk vendors: Review access logs for anomalies.

**8. Roles & Responsibilities**

| **Role** | **Responsibilities** |
| --- | --- |
| **Vendor Risk Officer (VRO)** | Oversees risk tier classification and audit scheduling. Reports to CISO. |
| **SOC Team** | Monitors vendor-related alerts in Splunk and coordinates incident response. |
| **Procurement Manager** | Ensures contracts include Premier’s security clauses before signing. |
| **Legal Team** | Enforces liability terms and manages breach notifications. |

**9. Compliance & Enforcement**

* **Non-Compliance Penalties**:
  + **Vendors**:
    - 1st offense: Mandatory remediation plan (30-day window).
    - 2nd offense: 5% contract value fine + quarterly audits.
    - 3rd offense: Termination.
  + **Internal Teams**: Compliance failures escalate to department heads and HR.
* **Documentation**: All records stored in Premier’s *Microsoft SharePoint ISMS repository*.