Third-Party Risk Management Policy

Purpose

We-Bond Solutions utilizes third-party products and services to support our mission and goals. This Third-Party Information Security Risk Management Policy establishes a consistent framework for identifying, assessing, monitoring, and managing risks associated with these third-party relationships. It ensures that vendors and suppliers meet appropriate security, compliance, and operational standards before and during engagement.

Scope

This policy applies to all individuals who, on behalf of We-Bond Solutions, engage with all third parties that provide services, systems, or solutions, including vendors, contractors, consultants, and service providers with access to company data, systems, or facilities.

It is intended for all relevant stakeholders, including Procurement, Legal & Compliance, Information Security, Risk Management, and Business Units involved in third-party engagements.

Definitions

The following definitions apply only to aid the understanding of the reader of this policy:

Employee:	A part-time or full-time individual employed by We-Bond Solutions.
Third Party/3rd Party:	Any external person or organization that provides services, systems, software, or products to We-Bond Solutions and is not an employee.
Critical Vendor:	A third party whose failure or compromise could significantly impact operations, data confidentiality, or regulatory compliance.
Information Resource:	Any system, service, or asset involved in the creation, use, management, storage, or destruction of We-Bond Solutions' information.
Inherent Risk:	The level of information security risk related to the nature of a third-party relationship before considering mitigating controls. Sometimes referred to as "impact."
Residual Risk:	The level of information security risk that remains after applicable protections and controls have been applied and evaluated.
Risk Tier:	A classification (High, Medium, Low) assigned based on the risk of the third party. It guides the level of due diligence required.

Due Diligence:	The process of evaluating a third party's security, privacy, compliance, and operational controls prior to or during engagement.

Roles & Responsibilities

TPRM Program Owner:	Oversees the third-party risk management program, maintains policies and processes, and ensures alignment with regulatory and security requirements.
Business Units:	Identify third-party needs, initiate engagement requests, and ensure timely participation in the TPRM process.
Procurement:	Coordinates vendor onboarding in line with policy requirements and ensures contracts include appropriate risk and security terms.
Information Security:	Conducts security risk assessments, reviews documentation and evidence, and classifies risk tiers.
Legal & Compliance:	Reviews contracts for compliance with regulatory obligations and advises on risk-related terms and waivers.
Third Parties:	Respond to due diligence requests, provide required documentation, and implement agreed-upon security or compliance remediation.

Policy

We-Bond Solutions requires that all third-party relationships undergo formal, risk-based due diligence before onboarding and throughout the engagement lifecycle. This policy establishes mandatory practices for identifying, assessing, mitigating, and monitoring inherent and residual risks, including but not limited to information security, financial risk, reputational exposure, and supply chain dependency.

A. Risk Assessments

- All third parties with access to We-Bond Solutions' Information Resources must:
  - Sign a Third-Party Non-Disclosure Agreement (NDA)
  - Sign a Service/License Agreement, where applicable
- Prior to engagement, all third-party relationships must undergo an inherent risk assessment to determine the baseline risk level associated with:
  - Access to company systems, data, or networks
  - Sensitivity of data processed (e.g., PII, PHI, PCI)
  - Criticality of the service or business function

    - Financial health indicators (e.g., creditworthiness, funding, solvency)
    - Reputational risk factors (e.g., past breaches, litigation, media presence)
    - Supply chain concentration or geopolitical exposure
- Inherent risk must be classified as High, Medium, or Low using standardized tiering criteria.
- Inherent risk must be re-evaluated at least bi-annually, and upon any of the following:
    - Material changes in services or data usage
    - Corporate acquisitions, divestitures, or restructuring
    - Reported incidents, non-compliance, or audit failures
    - Observations from Open-Source Intelligence (OSINT) feeds or threat intelligence platforms
- For third parties classified as High or Medium risk, a residual risk assessment must be conducted using:
    - Completed due diligence questionnaires
    - Supporting artifacts (e.g., SOC 2 Type II, ISO/IEC 27001, HIPAA attestations, risk register)
    - OSINT sources including data breach databases, regulatory actions, adverse media screening, litigation records, vendor reputation scoring
    - Technical assessments or tools (e.g., attack surface monitoring, vulnerability rating services)
    - Third-party risk intelligence services or external scorecards
    - Financial analysis and risk of insolvency
    - Assessment of supply chain controls, sub-tier vendors, and service continuity
- Residual risk assessments must evaluate:
    - Administrative, technical, and physical controls
    - Compliance maturity and control effectiveness
    - Ability to respond to incidents or crises
    - Downstream or fourth-party risk impact
- Risk thresholds must be defined for residual risk acceptance. Third parties that fail to meet risk tolerance levels must:
    - Be rejected or offboarded, or
    - Undergo remediation or re-scoping to reduce exposure, or
    - Be submitted for executive-level risk acceptance via waiver with documented justification and time-bound conditions

- Regulated third parties (e.g., those subject to HIPAA, PCI-DSS, GDPR) must be reassessed annually at minimum.

B. Third-Party Management Requirements

- All third-party agreements must include clauses addressing:
    - Authorized access to company data or systems
    - Data protection expectations, encryption requirements, and retention periods
    - Methods of data exchange and transfer
    - Secure return, destruction, or disposal of company data at end of contract
    - Minimum control requirements aligned to ISO 27001, NIST CSF, or relevant regulatory frameworks
    - Incident response timelines and escalation obligations
    - We-Bond Solutions' right to audit, assess, or request third-party assurance (e.g., audits, certifications)
- Subcontractor use must be disclosed and controlled:
    - Prime vendors are responsible for managing fourth-party risk
    - Subcontractors must meet equivalent security, financial, and compliance standards
- Vendors must:
    - Use Information Resources only for authorized purposes
    - Seek written approval for work outside defined contract parameters
    - Report all security, operational, financial, or reputational incidents immediately to their assigned point of contact
- Performance Monitoring:
    - Vendor performance must be reviewed at least annually, including:
        - SLA compliance
        - Control performance
        - Emerging risk indicators
        - Financial standing or credit changes
        - Public disclosures or OSINT alerts
    - Regular follow-up meetings are required for non-compliance until resolution or offboarding
- Operational Oversight:
    - Major third-party activities must be logged and available upon request, including:

        - Password resets, staff turnover, major project milestones, deliverables, and access records
    - Third parties must:
        - Provide and maintain an accurate list of key personnel
        - Notify We-Bond Solutions within 24 hours of key staff changes
        - Return or destroy sensitive materials upon employee separation or reassignment
        - Be reminded of confidentiality and NDA obligations post-engagement
        - Surrender all access cards, devices, or assets at contract termination
        - Retain only approved equipment as documented by We-Bond Solutions IT.

Waivers

If a third party cannot meet We-Bond Solutions' residual risk thresholds or policy requirements after due diligence and attempted remediation, a formal waiver may be requested.

Waiver requests must include:

- The unmet requirement and specific residual risk
- Business justification and any compensating controls
- An expiration or review date
- Sign-off from the risk owner and business sponsor

Approvals must be obtained from:

- TPRM Program Owner
- Information Security and Risk Management
- Legal & Compliance (if regulatory/contractual impact exists)
- An **executive sponsor** (e.g., CIO, CISO, General Counsel, CRO)

Waiver management requirements:

- Stored in the vendor's risk file
- Reviewed **annually** or immediately upon major changes (e.g., incidents, service scope)
- Re-evaluated or rescinded upon expiration; no open-ended waivers permitted

Enforcement

This Third-Party Information Security Risk Management Policy complements all other We-Bond Solutions information security policies and does not supersede them. Any perceived or actual conflicts between policies must be reported immediately for resolution.

Non-compliance by internal staff or third parties may result in corrective action, including revocation of access, disciplinary measures, contract suspension or termination, and, where applicable, civil or criminal penalties.

We-Bond Solutions reserves the right to audit, escalate, or enforce actions necessary to maintain compliance and mitigate risk.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2024	September, 2024	James Smith, CISO	Document Origination