1.10 OUTSOURCING AND THIRD-PARTY SERVICE PROVIDERS

1. Purpose
This policy outlines the principles, guidelines, and procedures for VIPCo's management of risks related to outsourcing and third-party service providers. It aims to ensure that outsourcing arrangements enhance operational efficiency while maintaining the VIPCo's accountability for its business activities and services. The policy is in accordance with the OSFI's Third-Party Risk Management Guideline.

2. Scope
This policy applies to all outsourcing arrangements and third-party service providers, including consultants, technology providers, and other external entities supporting VIPCo's operations, regardless of geographical location.

3. Governance and Accountability

- VIPCo retains full accountability for all outsourced services and remains responsible for risk management, including data protection, regulatory compliance, and service quality.
- Senior management is responsible for ensuring that third-party arrangements align with the firm's business strategy and risk appetite.
- A **Third-Party Risk Management Framework (TPRMF)** will be developed, outlining clear roles and responsibilities for managing and mitigating risks across the lifecycle of third-party relationships.

4. Risk-Based Approach

- **Due Diligence**: Before entering any agreement, conduct due diligence based on the criticality and risk level of the third-party. This includes financial stability, operational resilience, data security, and compliance with applicable laws.
- **Subcontracting Risk**: Third parties should provide transparency around subcontractors, and the firm must monitor risks arising from subcontracting arrangements.

5. Contracts and Written Agreements

- All third-party arrangements should be formalized in written contracts, which clearly define the rights, responsibilities, and service levels. Contracts for high-risk arrangements should include provisions on data security, business continuity, and termination rights.
- Where no written agreement is feasible, VIPCo will employ alternative monitoring and contingency measures.

6. Business Continuity and Exit Strategy

- Critical third-party service providers must establish business continuity and disaster recovery plans, which should be tested regularly. Evidence of this to be provided in the format of an annual. System and Organization Controls (SOC) Report.

- An exit strategy is developed for all critical services, outlining how VIPCo will transition to alternative providers or bring services in-house in the event of service disruptions to crucial providers.

7. Monitoring and Auditing

- VIPCo will periodically audit third-party performance and compliance with contractual obligations.
- Metrics and key risk indicators (KRIs) will be established to ensure that risks remain within acceptable thresholds, with senior management involved in escalation procedures as needed.

8. Technology and Cyber Risk Management

- Third parties with access to sensitive data or critical IT infrastructure must adhere to the VIPCo's technology and cyber standards, as well as recognized industry standards.
- Special attention is given to cloud service providers, ensuring portability and security measures are in place.

9. Incident Management

- Third-party providers must have documented processes for managing and escalating incidents, particularly in relation to data breaches, cyber threats, and service disruptions.
- VIPCo requires timely reporting of all incidents and work with third parties on remediation and root cause analysis.

10. Compliance with OSFI Guidance

This policy must be read by employees engaging with third party service providers and applied in conjunction with relevant OSFI guidelines, including but not limited to B-13 (Technology and Cyber Risk Management) and other applicable regulations.

11. Review and Continuous Improvement

- This policy, as well as the TPRMF, will be reviewed and updated regularly by the CCO to ensure it remains relevant and effective.
- Lessons learned from third-party incidents and audit findings will be incorporated into ongoing risk management practices.