Vendor Management Policy - Control Implementation Checklist

To ensure that all security policies requirements are consistently implemented, monitored, and maintained, the following checklist has been developed. It translates specific policy controls into actionable tasks, assigns clear ownership, and establishes tracking mechanisms to support ongoing compliance and operational effectiveness.

Policy Reference	Control Description	Frequency	Evidence Required	Status	Note
Vendor Management Policy	Conduct information security due diligence on all new vendors prior to engagement	As required	Assessment report		
	Conduct Environmental, Social, and Governance (ESG) due diligence on all new vendors prior to engagement	As required	Assessment report		
	Document the vendor assessments, including identified risks and action items.	As required	Assessment report, risk register, risk meeting minute		
	Reassess risks and update contracts and vendor inventories accordingly.	Annually/ As required	Updated information		
	Send security questionnaires	Prior to engagement	Filled questionnaires		

		/ As required			
	Include relevant security and privacy requirements in the contract. e.g: -Data security and compliance -Regular security reviews and independent validations. -Incident management, data breach notification, data return, or destruction upon contract termination. -Training requirements and intellectual property protection. -Geographic limitations -Notification of subcontractor/subprocessor changes	Prior to engagement / during renewal	Contracts/agreements containing security clauses		
	Include screening and background checks for vendor personnel (if applicable)	TBD			If applicable
	Maintain a vendor registry complete with risk level, types of data shared, service description and primary contacts.	On going	Vendor register with the required information		
	Review critical vendors' compliance reports (e.g., SOC 2, ISO 27001) and document findings.	Annual	Documented findings		

	Audit vendors periodically (if applicable)	As required	Audit findings		
	Monitor vendor activities, including access logs and service-level agreements (SLAs).	TBD			Can use monitoring tools if applicable.
	Document and track all vendor-related incidents, resolutions, and lessons learned.	On going	Information included in the vendor register		
	Manage changes through Change Management in vendor services e.g. system upgrades, new technologies, or physical relocations.	On going	Change Management records		
Logging and Monitoring Policy					