The World Bank Group

Information Security Compliance Questionnaire for External Service Providers

1. The questions below must be answered by the prospective External Service Provider prior to signing a contract for service provision. All responses must include and accurately reflect those of all sub-contractors and other third parties that provide services related to the overall engagement (e.g. infrastructure). Satisfactory answers will comply with the Bank Group's Information Security Policies.

2. The sponsoring Business Unit Manager is responsible for ensuring that this questionnaire is completed and verified. The Office of Information Security will provide advice as requested by the Business Unit Manager.

Serial #	Question	Yes	No	Comments
	Do you have documented information security policies and procedures? If yes, what national or international standards are they based on?	X		Based on ISO 27002
	Have the security controls in your organization been recently assessed by an independent third party in accordance with an industry accepted standard (i.e. SOC1 or SOC2 report)? Please provide details.		X	
	Do you conduct thorough security background checks including but not limited to personal reference checks, employment record verification, and criminal background checks for your employees?	X		
	Do you have documented Business Continuity Plans? Please provide details on the plan and your backup processes.	X		All digital assets are backed up into cloud on daily basis. Based on ISO 27002
	If yes to above, are your Business Continuity Plans based on any national or international standards? Please provide details of the standard.	X		
	Do you agree to return all World Bank Group information in your possession upon termination of the contract?	X		
	Do you have documented change management procedures?	X		Based on ISO 27002
	Do you have documented configuration management procedures?	X		Based on ISO 27002

Serial #	Question	Yes	No	Comments
	Do you employ user access management tools? Please provide details.	X		We employ single-sign-on frameworks, e.g OpenAuth providers and public keys
	Do you use malicious code and/or virus protection systems? Please provide details.	X		Avast anti-virus on all workstations
	Do you have documented patch management procedures? Please provide details.	X		Jira, Tewamworks, and Bitbucket for bugs reporting. Patches applied through and stored in version control systems such as cvs and/or git.
	Do you have systems to monitor the availability, usage and response time for applications?	X		We utilize cloud-based services that guaranty 99.99% availability. Google Analytics is used for monitoring the usage and the response time. For monitoring we use cloud- based availability monitoring services (monitor.us, monitis.com)
	Do you employ filtering technologies to isolate each customer's network connectivity from others?	X		We use separate virtual machines to completely isolate customers.
	Do you employ physical access controls for your data center? Please provide details.	X		24-hour security at hosting facility.
	Do you use environmental protection controls and infrastructure to adequately protect systems holding Bank data? Please provide details.	X		The hosting facility relies on two unique independent power feeds. In additional to multiple power feeds, all data centers have their own power generators and enterprise-class UPS technology.
	Will you collect, maintain and make available to the World Bank relevant security and access logs including server and security device logs (firewall/WAF)?	X		

Serial #	Question	Yes	No	Comments
	In order to assess the security of World Bank websites, we plan to perform vulnerability scanning at the application and infrastructure layer using automated tools before the site goes live and regularly after the site is in production. Do we have your permission to perform these scans? If not, please provide a reason. (We will perform OWASP 10 vulnerability scans before the application is moved to production; regular scans in production are scaled down non-intrusive vulnerability scans.)	X		
	Are there any specific days of the week and times of the day that we should NOT scan? If so, please list those days and times in the comments.	X		

I, the undersigned, certify that I am a duly authorized officer or representative of ___ECTOSTAR INC.__ (Company Name), and that all of the answers and statements made on this form are true and complete in every respect to the best of my knowledge and belief.

______________________________	CEO ______________________________
Signature of Authorized Officer	Title
VAHAN AMIRBEKYAN ______________________________	MAY 20, 2023 ______________________________
Printed Name	Date