GP PARSIK SAHAKARI BANK LTD.

Third-Party Security Assessment

Vendor Name: .

Services Rendered:

Questionnaire Instructions: The following questions are a set of multi-part questions. If any part(s) of the question are no or N/A please fill in No or N/A in the response field.
If No or N/A has been chosen then it is mandatory to supply additional explanation. Use the "Notes" field to the right of the question.

Number	Question	Response Y/N	Notes - Remark
A.	**Risk Management**		
1	Does your organization have a formal (documented and implemented) risk assessment program with an owner assigned for maintenance and review of the program?		
2	Does the program periodically review accepted risk?		
B.	**Security Policy**		
3	Does your organization have formal (documented and implemented) information security policies and procedures that are approved by senior management?		
4	Does your organization have formal (documented and implemented) information security policies and procedures that have provisions for disciplinary actions for noncompliance?		
5	Does your organization have formal (documented and implemented) information security policies and procedures that are reviewed at least annually?		
C.	**Organizational Security**		
6	Does your organization have an Information Security Oversight function which has an individual or group responsible for the program, who is/are responsible for ensuring compliance with security policies?		
7	Are all constituents required, upon hire, to sign a Code of Ethics or any agreement(s) that require non-disclosure, preservation of confidentiality, and/or acceptable use?		
8	For all Dependent Service Providers with access to target data, is there a process in place to regularly monitor compliance with security standards?		
D.	**Asset Management**		
9	Does your organization have a formal (documented, approved, published, communicated and implemented) asset management program which includes a complete list of all hardware and software assets?		
10	Does your organization have a formal (documented, approved, published, communicated and implemented) asset management program which has an owner responsible for approving and reviewing access to the assets?		
11	Does your asset management program address the treatment, handling, disposal, destruction and reuse of media / assets that contain target data?		
12	Does your organization have a formal (documented, approved, published, communicated and implemented) information classification policy?		
E.	**Human Resource Security**		
13	Does your organization perform background screening of applicants to include prior employment, criminal, credit, professional, academic, references and drug screening (unless prohibited by law)?		
14	Are constituents required to undergo information security awareness training upon hire?		
15	Does your organization have a formal (documented, approved, published, communicated and implemented) asset return policy governing all company-owned assets from either terminated constituents or constituents who change status?		
F.	**Physical and Environmental Security**		
16	Does your organization have a formal (documented, approved, published, communicated and implemented) Physical Security Policy?		
17	Are all visitors are signed in / logged prior to entering sensitive facilities (where target data is stored, processed or viewed):		
18	Are all visitors are required to provide government issued ID prior to entering sensitive facilities (where target data is stored, processed or viewed):		
19	Are all visitors escorted at all times and required to wear clearly identifiable visitor credentials in sensitive facilities (where target data is stored, processed or viewed):		
20	Is physical access into sensitive facilities (where target data is stored, processed or viewed) protected by security guards?		
21	Is physical access into sensitive facilities (where target data is stored, processed or viewed) protected by electronic access devices?		
22	Is physical access into sensitive facilities (where target data is stored, processed or viewed) protected by bio-metric access devices?		
23	If physical access into sensitive facilities (where target data is stored, processed or viewed) is protected, are access lists periodically reviewed?		
24	Has your organization deployed a CCTV to monitor access to all sensitive areas (where target data is stored, processed or viewed)?		
25	If your organization has deployed a CCTV to monitor access to all sensitive areas (where target data is stored, processed or viewed), is the CCTV video stored or archived for 90 days or greater?		
G.	**Communications and Operations Management**		

26	Does your organization have a formal (documented, approved, published, communicated and implemented) Change Control / Change Management process that contains approval for all changes and logs all changes?		
27	Do all systems and workstations have antivirus software which is installed and configured to scan the system?		
28	Do all systems and workstations have antivirus software which is periodically updated (including scan engine and signatures)?		
29	Do all systems and workstations have antivirus software which is configured so users cannot disable the scans?		
30	Do all external network connections terminate on a firewall configured with a 'deny all' rule?		
31	Do you allow telnet, FTP or any other unsecured protocol into or out of your network?		
32	Are all network and system devices configured so that system errors and security events are logged?		
33	Are all network and system devices configured so that logs are protected from alteration by the users?		
34	Are all network and server devices and workstations (that process, store or view target data) built according to a standard configuration process?		
35	Are these devices periodically reviewed for deviations to the standard configuration?		
36	Are all servers, workstations, applications, and/or network devices (that process, store or view target data) patched on a regular basis?		
37	Are all external network connections monitored by an IPS/IDS or other network monitoring tool that generate alerts when a security event is detected?		
38	And are the alerts acted on according to a response time based on severity level?		
39	Does your organization have a formal (documented, approved, published, communicated and implemented) Wireless Network policy / process mandating strong encryption?		
40	Does your organization have a formal (documented, approved, published, communicated and implemented) Wireless Network policy / process mandating non-broadcast of SSID?		
41	Does your organization have a formal (documented, approved, published, communicated and implemented) Wireless Network policy / process mandating two factor authentication?		
42	Is encryption implemented for all target data, both electronic transmissions and physical electronic media, prior to sending outside of your environment?		
43	Does your organization have a formal (documented, approved, published, communicated and implemented) Physical Media policy / process which includes limiting approved access to physical media devices (USB, CDR, DVDR, floppy, backup tape, etc.)?		
44	Does your organization have a formal (documented, approved, published, communicated and implemented) Physical Media policy / process which includes disposal of media?		
H.	**Access Control**		
45	Does your organization have a formal (documented, approved, published, communicated and implemented) Access Control policy/process to include role based access to all resources (applications, OS, network devices, etc.)?		
46	Does your organization have a formal (documented, approved, published, communicated and implemented) Access Control policy/process to include a unique ID for all individuals?		
47	Does your organization have a formal (documented, approved, published, communicated and implemented) Access Control policy/process to restrict or remove the use of generic IDs (guest, administrator, root, etc.)?		
48	Does your organization have a formal (documented, approved, published, communicated and implemented) Access Control policy/process to include prohibition on sharing of IDs?		
49	Does your organization perform annual (or more frequent) reviews of access rights to systems, applications and network devices?		
50	Does your organization have a formal (documented, approved, published, communicated and implemented) Password policy / process that includes prohibition on sharing passwords?		
51	Does your organization have a formal (documented, approved, published, communicated and implemented) Password policy / process that includes requirement for passwords to be changed at initial logon?		
52	Does your organization have a formal (documented, approved, published, communicated and implemented) Password policy / process that includes a requirement for periodic subsequent password changes?		
53	Does your organization have a formal (documented, approved, published, communicated and implemented) Remote Access / Teleworking policy / process that requires multifactor authentication for access to all systems, applications or network devices from all remote access devices (laptop, home PC, PDA, etc.)?		
I.	**Information Systems Acquisition Development and Maintenance**		
54	Does your organization have a formal (documented, approved, published, communicated and implemented) System Development Lifecycle policy / process that includes application development and testing?		
55	Does your organization have a formal (documented, approved, published, communicated and implemented) Vulnerability Assessment policy / process, and does it require vulnerability assessments on all systems, applications and network devices that access / process / or store target data?		
56	Does your organization have a formal (documented, approved, published, communicated and implemented) Vulnerability Assessment policy / process, and does it classify issues according to severity?		
57	Does your organization have a formal (documented, approved, published, communicated and implemented) Vulnerability Assessment policy / process, and is there a requirement to remediate all issues which are considered high-risk?		

58	Does your organization perform annual (or more frequent) penetration tests of all Internet-facing applications?		
59	If any high risk issues are identified, are they corrected within 90 days?		
J.	**Information Security Incident Management**		
60	Does your organization have a formal (documented, approved, published, communicated and implemented) Incident Response policy / process / plan that includes requirements to report all potential incidents?		
61	Does your organization have a formal (documented, approved, published, communicated and implemented) Incident Response policy / process / plan that includes testing of the plan?		
62	Does your organization have a formal (documented, approved, published, communicated and implemented) Incident Response policy / process / plan that includes notification to clients in the event of a breach?		
63	Does your organization have a formal (documented, approved, published, communicated and implemented) Incident Response policy / process / plan that includes an incident response team with clearly defined roles?		
K.	**Compliance**		
64	Is your organization required to comply with any legal, regulatory or industry, requirements, etc. (GLBA, SOX, PCI, SEC)?		
65	Within the last year, has there been an independent review of your organization's security policies, standards, procedures, and/or guidelines?		
			AVERAGE