The Nainital Bank Ltd.
(Regd. Office: G. B. Pant Road, Nainital)

Solution For Managing Internet Endpoints Across Branches and Administrative Offices			
Technical Specifications & Core Features			
General			
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
1	The Solution must be SaaS based		
2	The Solution must have management as Cloud-hosted, web based, consolidated for all services		
3	OEM should commit 99.999% of SLA uptime of the service on written or public document for SASE/SSE		
4	The Solution should support infrastructure as code using Terraform.		
5	The Solution should support API to configure and manage Networks, Gateways, Regions, Users, Groups, Tunnels, etc		
6	The Solution should have at least 70+ POP's globally and minimum 6 in India		
7	The Solution must provide dedicated static public IP address to the tenant/gateway without any cost or license.		
Deployment			
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
8	The Solution should support operating system like Windows, MAC, Linux, Ubuntu, Red hat, Android, Chromebook, IOS, etc for private access and Windows, Linux and MAC for Internet access		
9	The licensing should be on number of users not devices. Assuming User may use multiple devices		
10	Each user should be able to use up to 5 devices with the same license		
11	Admin should be able to control agent's version updates		
12	Client software should auto-update on user devices directly based on policy		
Integration			
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
	The Solution/platform should support Azure AD, Okta, Local AD, and any SAML 2.0 identity provider for authentication as an IDP		
	The Solution should support platform for guest users (email and password) and multi-factor authentication (MFA)		
	Simultaneous support of Internal/local DB users (for third party/contractors) and IDP integrated users.		
	The Solution should support Identity group integration/Synchronization		
	The Solution should have SCIM integration capabilities with Azure AD and Okta		
Internet Access			
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
	Platform must support split tunnelling, including both include/exclude options and support for both IP and FQDN		
	The solution support Internet access directly through On-Device network protection without routing all the traffic to POP		
	Solution must have inbuilt categories to select/provide access to the selected users/groups, etc. Should be able to create custom URL if required by business		
	There should be an option to bypass rule to exclude scanning for trusted domains like Microsoft, google drive, etc		

	Internet access solution supports accurate localized web content even in the cities without local POP infrastructure		
	Local agent must support SWG functionality even when the client disconnects from the VPN		
	SWG functionality should support HTTPS inspection. Inspection must be performed directly on the agent in order to keep user privacy		
	Client based access provides automated secure access over unprotected Wi-Fi network (when unprotected Wi-Fi network is detected, client must route all traffic via VPN even when split tunnelling is defined)		
	Browsing Security		
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
	Supported Browsers: Chrome, Edge, Firefox, Safari		
	The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content.		
	When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox		
	Incoming files will be emulated by sandboxing for potentially malicious content.		
	The solution will detect zero-day phishing sites that request user credentials even if unknown to reputation engines.		
	The solution must block the user from browsing to a known malicious URLs or domains.		
	The solution must block the user from using its corporate credentials in a site that does not belong to the corporate domain.		
	The solution must have the option to block artificial intelligence sites.		
	The solution must enforce "Safe Searching" feature when they employ the Google, Bing and Yahoo search engines		
	DLP		
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
	The solution should provide upload and download protection to and from cloud services.		
	The solution should provide predefined data types to be used as well as the option to customize data types to be allowed\blocked.		
	The solution should support creating policies based on data formats to be allowed/blocked.		
	The solution should provide a text scan on AI platforms to prevent data leak to AI databases.		
	The solution should provide complete visibility of the DLP insights and events.		
	The solution should provide clipboard control, copy-paste, print and save restrictions		
	The solution should allow data type grouping to improve user experience in setting policies.		
	Compliance and Security		
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
	The OEM should comply to global certification like SOC2 Type 2, GDPR, ISO, etc		
	Policies should be based on users, groups, IP objects, FQDN, ports, and services		
	The solution should be able to create policy or posture profiling based on different category of users.		

	The Solution must provide details on device inventory capabilities, including visibility of connected devices, posture status, serial number, location, and online/offline status.		
Posture Management			
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
	The Solution should Support Posture Check options for Windows OS: OS version, Certificate, running process, running Antivirus, File existence, Disk encrypted, Registry key, AD association, Windows Security Center firewall and AV registered		
	The Solution should Support Posture Check options for MAC OS: OS version, Certificate, running process, running Antivirus, File existence, Disk encrypted		
	The Solution should Support Posture Check options for Linux OS: Running process, running Antivirus, File existence		
	The solution should support client less posture check. This must al least include date and time, Geo location, location Ip, OS, Browser, etc.		
	Agent-less applications must allow to define multiple applications for the same target server/machine with different access credentials		
	Agent-less applications can be defined with private domain aliases for user-friendly access		
	Certificate Management: The Solution must allow too manage domain certificates for domain-associated user friendly access to agent-less applications		
	The Solution should have feature to perform regular posture check (e.g. Every 20-30 mins)		
Logging and Monitoring			
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
	Solution should have logging capabilities, including audit, policy, and user session logs.		
	Must provide information on how member activities and sessions are tracked.		
	Reporting capabilities should display for compliance status and malware detection.		
Compliance			
Sr. No.	**Particulars**	**Compliance (Yes/No)**	**Remarks**
	OEM MAF is required		