TECHNICAL EVALUATION OF MULTIMEDIA PROJECTOR

Sl No.	Peripherals	Specifications	Firms		
			1	2	3
			M/s egs (PVT.) Ltd.	Paper Communication (PVT.) Ltd.	Al-Khair Traders
1	**Brand**	Renowned Brand	Panasonic PT-LRZ 35	Panasonic PT-LRZ 35	Panasonic PT-LRZ 35
2	Projector type	1-Chip DLP™ projector	1-Chip DLP™ projector	1-Chip DLP™ projector	1-Chip DLP™ projector
3	Panel size	17.0 mm (0.67 in) diagonal, 16:10 aspect ratio	17.0 mm (0.67 in) diagonal, 16:10 aspect ratio	17.0 mm (0.67 in) diagonal, 16:10 aspect ratio	17.0 mm (0.67 in) diagonal, 16:10 aspect ratio
4	Display method	DLP™ chip x 1, DLP™ projection system	DLP™ chip x 1, DLP™ projection system	DLP™ chip x 1, DLP™ projection system	DLP™ chip x 1, DLP™ projection system
5	Number of pixels	2,304,000 (1920 x 1200) pixels	2,304,000 (1920 x 1200) pixels	2,304,000 (1920 x 1200) pixels	2,304,000 (1920 x 1200) pixels
6	Light source	Light Emitting Diode	Light Emitting Diode	Light Emitting Diode	Light Emitting Diode
7	Light output	3,500 lm or above	3,500 lm or above	3,500 lm or above	3,500 lm or above
8	Time until light output declines to 50 %***2**	20,000 hours or above	20,000 hours or above	20,000 hours or above	20,000 hours or above
9	Resolution	1920 x 1200 pixels	1920 x 1200 pixels	1920 x 1200 pixels	1920 x 1200 pixels
10	Contrast ratio	30,000:1 (When [Light power] is set to [Normal] and [Picture Mode] is set to [Dynamic])	30,000:1 (When [Light power] is set to [Normal] and [Picture Mode] is set to [Dynamic])	30,000:1 (When [Light power] is set to [Normal] and [Picture Mode] is set to [Dynamic])	30,000:1 (When [Light power] is set to [Normal] and [Picture Mode] is set to [Dynamic])
11	Screen size [diagonal]	1.02–7.62 m (40–300 in), 16:10 aspect ratio	1.02–7.62 m (40–300 in), 16:10 aspect ratio	1.02–7.62 m (40–300 in), 16:10 aspect ratio	1.02–7.62 m (40–300 in), 16:10 aspect ratio
12	Center-to-corner zone ratio	90%	90%	90%	90%
13	Lens	1.3x manual zoom (throw ratio: 1.28–1.69:1)	1.3x manual zoom (throw ratio: 1.28–1.69:1)	1.3x manual zoom (throw ratio: 1.28–1.69:1)	1.3x manual zoom (throw ratio: 1.28–1.69:1)
14	Lens shift (From the origin point of the lens mounter)	Vertical: +50 %, +40 %	Vertical: +50 %, +40 %	Vertical: +50 %, +40 %	Vertical: +50 %, +40 %
15	Keystone correction range	Vertical: ±30 °	Vertical: ±30 °	Vertical: ±30 °	Vertical: ±30 °
16	Installation	Ceiling/floor, front/rear, 2-axis 360-degree installation	Ceiling/floor, front/rear, 2-axis 360-degree installation	Ceiling/floor, front/rear, 2-axis 360-degree installation	Ceiling/floor, front/rear, 2-axis 360-degree installation
17	HDMI IN 1/HDMI IN 2	HDMI 19-pin x 2 (HDCP and Deep Color compatible), CEC supported	HDMI 19-pin x 2 (HDCP and Deep Color compatible), CEC supported	HDMI 19-pin x 2 (HDCP and Deep Color compatible), CEC supported	HDMI 19-pin x 2 (HDCP and Deep Color compatible), CEC supported
18	COMPUTER 1 IN	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)
19	COMPUTER 2 IN	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)
20	COMPUTER OUT	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)	D-sub 15-pin (female) x 1 (RGB/YPBPR/YCBCR)
21	VIDEO IN	Pin jack x 1	Pin jack x 1	Pin jack x 1	Pin jack x 1
22	AUDIO 1 IN/AUDIO 2 IN	M3 stereo mini-jack x 2	M3 stereo mini-jack x 2	M3 stereo mini-jack x 2	M3 stereo mini-jack x 2
23	VARIABLE AUDIO OUT	M3 stereo mini-jack x 1	M3 stereo mini-jack x 1	M3 stereo mini-jack x 1	M3 stereo mini-jack x 1
24	SERIAL IN	D-sub 9-pin (female) x 1 for external control (RS-232C compliant)	D-sub 9-pin (female) x 1 for external control (RS-232C compliant)	D-sub 9-pin (female) x 1 for external control (RS-232C compliant)	D-sub 9-pin (female) x 1 for external control (RS-232C compliant)
25	LAN	RJ-45 x 1 for network control, 10Base-T, 100Base-T, compatible with PJ Link™ (Class 1)	RJ-45 x 1 for network control, 10Base-T, 100Base-T, compatible with PJ Link™ (Class 1)	RJ-45 x 1 for network control, 10Base-T, 100Base-T, compatible with PJ Link™ (Class 1)	RJ-45 x 1 for network control, 10Base-T, 100Base-T, compatible with PJ Link™ (Class 1)

Sl No.	Peripherals	Specifications	Firms		
			1	2	3
			M/s egs (PVT.) Ltd.	Paper Communication (PVT.) Ltd.	Al-Khair Traders
26	Micro USB	x 1 (for service use)	x 1 (for service use)	x 1 (for service use)	x 1 (for service use)
27	DC OUT	USB Connector (Type A) x 1 (for power supply, DC 5 V/2 A)	USB Connector (Type A) x 1 (for power supply, DC 5 V/2 A)	USB Connector (Type A) x 1 (for power supply, DC 5 V/2 A)	USB Connector (Type A) x 1 (for power supply, DC 5 V/2 A)
28	Power supply	AC 100–240 V, 50/60 Hz	AC 100–240 V, 50/60 Hz	AC 100–240 V, 50/60 Hz	AC 100–240 V, 50/60 Hz
29	Power consumption	NORMAL: 420 W, ECO: 255 W, QUIET: 196 W	NORMAL: 420 W, ECO: 255 W, QUIET: 196 W	NORMAL: 420 W, ECO: 255 W, QUIET: 196 W	NORMAL: 420 W, ECO: 255 W, QUIET: 196 W
30	Built-in speaker	10 W monaural	10 W monaural	10 W monaural	10 W monaural
31	Operation noise	NORMAL: 35 dB, ECO: 27 dB, QUIET: 24 dB	NORMAL: 35 dB, ECO: 27 dB, QUIET: 24 dB	NORMAL: 35 dB, ECO: 27 dB, QUIET: 24 dB	NORMAL: 35 dB, ECO: 27 dB, QUIET: 24 dB
32	Operating environment	Operating temperature: 0–40 °C (32–104 °F)*5; Operating humidity: 20–80 % (no condensation)	Operating temperature: 0–40 °C (32–104 °F)*5; Operating humidity: 20–80 % (no condensation)	Operating temperature: 0–40 °C (32–104 °F)*5; Operating humidity: 20–80 % (no condensation)	Operating temperature: 0–40 °C (32–104 °F)*5; Operating humidity: 20–80 % (no condensation)
33	Applicable software	Multi Monitoring & Control Software, Early Warning Software	Multi Monitoring & Control Software, Early Warning Software	Multi Monitoring & Control Software, Early Warning Software	Multi Monitoring & Control Software, Early Warning Software

Comments:

1 Three firms M/s egs (PVT.) Ltd. Paper Communication (Pvt.) Ltd. Ibd, and Al-Khair Traders have quoted technical specifications for Multimedia Projector.

2 All the stated firms fulfill tender specifications.

Recommendations:

Therefore, M/s egs (PVT.) Ltd. Paper Communication (Pvt.) Ltd. Ibd, and Al-Khair Traders are recommended for further proceedings, please.

TECHNICAL EVALUATION OF CARTRIDGE/TONER/HEADS AND PAPERS

Sl. No.	Functions / Peripherals	Specifications	Firms	
			1	2
			M/s Paper Communication, (Pvt) Ltd., Islamabad	M/s Jamal & Brothers Islamabad
1	HP 731 **Head Set** (HP T1708)		HP 731 Head Set of 3	HP 731 Head Set (HP T1708)
2	HP 72 **Ink Set** (HP T1708)		HP 72 Ink Set HP 72B 130 ml Photo Black Ink Cartridge HP 72 130 ml Cyan Ink Cartridge HP 72 130 ml Magenta Ink Cartridge HP 72 130 ml Yellow Ink Cartridge HP 72B 130 ml Gray Ink Cartridge HP 72B 130 ml Matte Black Ink Cartridge	HP 72 Ink Set (HP T1708)
3	HP 72 **Head Set** (HP T795)		HP 72 Head Set of 3	HP 72 Head Set (HP T795)
4	HP 72 **Ink Set** (HP T795)		HP 72 Ink Set of 6	HP 72 Ink Set (HP T795)
5	HP 82 **Ink Set** (HP 800 PS)		-	NA
6	HP 11 **Head** (HP 800 PS)		HP 11 Head Set C4210A HP No. 11 Black Printhead C4211A HP No. 11 Cyan Printhead C4212A HP No. 11 Magenta Printhead C4213A HP No. 11 Yellow Printhead	NA
7	HP **Ink Tonor** 81A (HP M605)		HP 81A Tonor	HP Tonor 81A (HP M605)
8	HP Color M750		HP 650A Tonor Set (Black, Cyan, Yellow, Magenta)	Tonor Set HP Color M750
9	HP Color CP 5225		HP 307A Tonor Set (Black, Cyan, Yellow, Magenta)	Tonor Set HP Color CP 5225
10	Paper Ream 80Gsm		Bright-white multi purpose office paper (BMO) ream of 500 sheets	Paper Ream A4 Size 80Gsm 500 sheets AA Brand
11	Glaxy Paper 24" 90 Gms		Glaxy Paper 24" 90 Gms	HP Coated Paper Q1404B 24" 90 Gms
12	Glaxy Paper 42" 90 Gms		Glaxy Paper 42" 90 Gms	HP Coated Paper Q1406B 42" 90 Gms
13	Canon Ir 3245		Canon NPG26 Toner	NA

Comments:

1 Two firms M/s Paper Communication, (Pvt) Ltd., Islamabad and M/s Jamal & Brothers Islamabad, have quoted technical specification for Cartridge/Toner/Heads and Papers.

2 M/s Jamal & Brothers, Islamabad has not qouted technical specifications against items mentioned at Sr. 5, 6 and 13 whereas M/s Paper Communication (Pvt) Ltd, has not quoted technical specifications against item at Sr. 5.

Recommendations:

Therefore, for the rest of the items, M/s Paper Communication (PVT), Ltd, and M/s Jamal & Brothers, Islamabad fulfill the technical specifications and recommended for further proceedings,

TECHNICAL EVALUATION OF ANTIVIRUS

Sl No.	Specifications	Firms	
		1	2
		M/s egs (PVT.) Ltd.	App in Snap (PVT.) Ltd.
1	Endpoint	Endpoint	Endpoint (Kaspersky)
2	Suggested endpoint solution must have Machine Learning Technologies	Kaspersky endpoint solution must have Machine Learning Technologies	Suggested endpoint solution have Machine Learning Technologies
3	The suggested solution must support high availability and clustering	Kaspersky support high availability and clustering	The suggested solution support high availability and clustering
4	The suggested solution must support secure communication between management server and endpoints	Kaspersky support secure communication between management server and endpoints	The suggested solution support secure communication between management server and endpoints
5	The suggested solution vendor must be in the “leaders” quadrant of Gartner’s latest magic quadrant report for at-least six years in a row.	Due to Russia War,US & European rating companies have stop evaluation of Russian technologies and products. Kaspersky is therefore not listed in Garter magic quadrants. Kaspersky is world known brand in Cyber Security System.	The suggested solution vendor is in the “leaders” quadrant of Gartner’s latest magic quadrant report for at-least six years in a row.
6	Suggested solution must support below client operating systems: Windows 7, 8, 8.1, 10 and windows 10 Red stone 1	Kaspersky support below client operating systems: Windows 7, 8, 8.1, 10 and windows 10 Red stone 1	Suggested solution support below client operating systems: Windows 7, 8, 8.1, 10 and windows 10 Red stone 1
7	Suggested solution must support below Server operating systems: Windows Server 2008, 2008 R2, 2012, 2012 R2 including standard, enterprise, core & datacenter editions. Windows Server 2016 essentials, standard, datacenter	Kaspersky support below Server operating systems: Windows Server 2008, 2008 R2, 2012, 2012 R2 including standard, enterprise, core & datacenter editions. Windows Server 2016 essentials, standard, datacenter	Suggested solution support below Server operating systems: Windows Server 2008, 2008 R2, 2012, 2012 R2 including standard, enterprise, core & datacenter editions. Windows Server 2016 essentials, standard, datacenter
8	Suggested solution must be able to detect following type of threats: Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-day vulnerabilities and other malicious and unwanted software	Kaspersky must be able to detect following type of threats: Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-day vulnerabilities and other malicious and unwanted software	Suggested solution is able to detect following type of threats: Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-day vulnerabilities and other malicious and unwanted software
9	Suggested solution must provide Memory Scanning for windows workstations	Kaspersky must provide Memory Scanning for windows workstations	Suggested solution provide Memory Scanning for windows workstations
10	Suggested solution must include following components in a single agent installed on the endpoint: a) Application, Web and Device control b) HIPS and Firewall	Kaspersky must include following components in a single agent installed on the endpoint: a) Application, Web and Device control b) HIPS and Firewall	Suggested solution must include following components in a single agent installed on the endpoint: a) Application, Web and Device control b)HIPS and Firewall
11	Suggest solution must include Application launch/start control for the windows server operating system.	Kaspersky solution must include Application launch/start control for the windows server operating system.	Suggest solution include Application launch/start control for the windows server operating system.
12	Suggest solution protection for servers must include dedicated component for the protection against ransomware/Cryptor viruses like activity on shared resources.	Kaspersky solution protection for servers must include dedicated component for the protection against ransomware/Cryptor viruses like activity on shared resources.	Suggest solution protection for servers must include dedicated component for the protection against ransomware/Cryptor viruses like activity on shared resources.
13	Suggested solution must have pre-defined list of scan exclusion for Microsoft applications and services.	Kaspersky solution must have pre-defined list of scan exclusion for Microsoft applications and services.	Suggested solution have pre-defined list of scan exclusion for Microsoft applications and services.
14	Suggested solution should support installation endpoint protection on Servers without restart	Kaspersky solution should support installation endpoint protection on Servers without restart	Suggested solution support installation endpoint protection on Servers without restart

Sl No.	Specifications	Firms	
		1	2
		M/s egs (PVT.) Ltd.	App in Snap (PVT.) Ltd.
15	Suggested endpoint solution must allow the following: a) Manual scanning b) On access scanning c) On demand scanning d) Compressed File Scanning e) Scan Individual file, Folder and drive f) Script blocking and scanning g) Auto clean, Quarantine infected files h) Registry guard i) Buffer Overflow Protection j) Instant messages (IM) scanning k) Background/idle scanning l) Removable drive scanning upon connection with the system m) Ability to detect untrusted hosts and block upon detection of encryption like activities on the server shared resources	Kaspersky endpoint solution must allow the following: a) Manual scanning b) On access scanning c) On demand scanning d) Compressed File Scanning e) Scan Individual file, Folder and drive f) Script blocking and scanning g) Auto clean, Quarantine infected files h) Registry guard i) Buffer Overflow Protection j) Instant messages (IM) scanning k) Background/idle scanning l) Removable drive scanning upon connection with the system m) Ability to detect untrusted hosts and block upon detection of encryption like activities on the server shared resources	Suggested endpoint solution allow the following: a) Manual scanning b) On access scanning c) On demand scanning d) Compressed File Scanning e) Scan Individual file, Folder and drive f) Script blocking and scanning g) Auto clean, Quarantine infected files h) Registry guard i) Buffer Overflow Protection j) Instant messages (IM) scanning k) Background/idle scanning l) Removable drive scanning upon connection with the system m) Ability to detect untrusted hosts and block upon detection of encryption like activities on the server shared resources
16	Suggested endpoint solution should be protected with a password to prevent stopping/killing the AV process and for self-protection regardless of user authorization level on the system	Kaspersky endpoint solution should be protected with a password to prevent stopping/killing the AV process and for self-protection regardless of user authorization level on the system	Suggested endpoint solution is protected with a password to prevent stopping/killing the AV process and for self-protection regardless of user authorization level on the system
17	Suggested solution must have local and global reputation	Kaspersky solution must have local and global reputation	Proposed solution have local and global reputation
18	Scans both HTTP and FTP traffic against viruses and spyware or any other malware.	Kaspersky Scans both HTTP and FTP traffic against viruses and spyware or any other malware.	Scans both HTTP and FTP traffic against viruses and spyware or any other malware.
19	Solution must include a personal firewall capable of, but not limited to: a) Block network activates of applications based on their categorization b) Block/allow certain packets, protocol, IP addresses, Ports and traffic direction c) Automatic and manual addition of network subnets and modify network activity permissions	Kaspersky solution must include a personal firewall capable of, but not limited to: a) Block network activates of applications based on their categorization b) Block/allow certain packets, protocol, IP addresses, Ports and traffic direction c) Automatic and manual addition of network subnets and modify network activity permissions	Solution include a personal firewall capable of, but not limited to: a) Block network activates of applications based on their categorization b) Block/allow certain packets, protocol, IP addresses, Ports and traffic direction c) Automatic and manual addition of network subnets and modify network activity permissions
20	The suggested solution must prevent the connection of reprogrammed USB devices that emulate keyboards and also allow to control the use of on screen keyboard for authorization.	Kaspersky solution must prevent the connection of reprogrammed USB devices that emulate keyboards and also allow to control the use of on screen keyboard for authorization.	The solution prevent the connection of reprogrammed USB devices that emulate keyboards and also allow to control the use of on screen keyboard for authorization.
21	Solution must be able to block network attacks and report the source of infection	Kaspersky must be able to block network attacks and report the source of infection	Solution is able to block network attacks and report the source of infection
22	Suggested solution have a proactive approach to prevent malwares from exploiting existing vulnerabilities	Kaspersky solution must have a proactive approach to prevent malwares from exploiting existing vulnerabilities	Solution have a proactive approach to prevent malwares from exploiting existing vulnerabilities
23	Suggested solution support signature based detection in addition to cloud-assisted and heuristics	Kaspersky solution support signature based detection in addition to cloud-assisted and heuristics	Solution must signature based detection in addition to cloud-assisted and heuristics
24	The proposed solution should have the ability to alert , clean, delete , quarantine the detected threats	Kaspersky solution should have the ability to alert , clean, delete , quarantine the detected threats	The proposed solution have the ability to alert , clean, delete , quarantine the detected threats

Sl No.	Specifications	Firms	
		1	2
		M/s egs (PVT.) Ltd.	App in Snap (PVT.) Ltd.
25	Solution should have the ability to accelerate scanning tasks skipping those objects that have not changed since the previous scan.	Kaspersky should have the ability to accelerate scanning tasks skipping those objects that have not changed since the previous scan.	Solution have the ability to accelerate scanning tasks skipping those objects that have not changed since the previous scan.
26	Suggest solution allow administrator to exclude specified files / folders / Application / By Digital Certificate from being scanned either in the on-access scan (real-time protection) or during on-demand scans.	Kaspersky solution must allow administrator to exclude specified files / folders / Application / By Digital Certificate from being scanned either in the on-access scan (real-time protection) or during on-demand scans.	Suggest solution allow administrator to exclude specified files / folders / Application / By Digital Certificate from being scanned either in the on-access scan (real-time protection) or during on-demand scans.
27	All detected threats (cleaned or active) be backed up in a central location where all samples can be re-examined or restored	All detected threats (cleaned or active) must be backed up in a central location where all samples can be re-examined or restored	All detected threats (cleaned or active) be backed up in a central location where all samples can be re-examined or restored
28	Automatically scans removable drives for malware upon insertion to any endpoint. Scan should be controlled based on drive size	Automatically scans removable drives for malware upon insertion to any endpoint. Scan should be controlled based on drive size	Automatically scans removable drives for malware upon insertion to any endpoint. Scan should be controlled based on drive size
29	Suggested solution must be able to block the usage of USB storage devices or only allow access to whitelisted devices and allow read/write access by domain users to reduce data theft and enforce lock policies	Kaspersky solution must be able to block the usage of USB storage devices or only allow access to whitelisted devices and allow read/write access by domain users to reduce data theft and enforce lock policies	Solution is able to block the usage of USB storage devices or only allow access to whitelisted devices and allow read/write access by domain users to reduce data theft and enforce lock policies
30	Suggested solution must be able to differentiate among USB storage devices, printers, mobiles and other peripherals	Kaspersky solution must be able to differentiate among USB storage devices, printers, mobiles and other peripherals	Suggested solution is able to differentiate among USB storage devices, printers, mobiles and other peripherals
31	Suggested solution must be able to log the file operations (Write and delete) on USB storage devices. Stated functionality does not require any additional license or component to installed on the endpoint.	Kaspersky solution must be able to log the file operations (Write and delete) on USB storage devices. Stated functionality does not require any additional license or component to installed on the endpoint.	Suggested solution is able to log the file operations (Write and delete) on USB storage devices. Stated functionality does not require any additional license or component to installed on the endpoint.
32	Suggested solution must have ability to block the execution of any executable from the USB storage device.	Kaspersky solution must have ability to block the execution of any executable from the USB storage device.	Suggested solution have ability to block the execution of any executable from the USB storage device.
33	Suggested solution must have a ability to generate list of trusted Wi-Fi networks based on name, encryption type and authentication type.	Kaspersky solution must have a ability to generate list of trusted Wi-Fi networks based on name, encryption type and authentication type.	Suggested solution have a ability to generate list of trusted Wi-Fi networks based on name, encryption type and authentication type.
34	Suggested solution must have Ability to block/allow user access to web resources based on websites, content type, user and time of day	Kaspersky solution must have Ability to block/allow user access to web resources based on websites, content type, user and time of day	Suggested solution have Ability to block/allow user access to web resources based on websites, content type, user and time of day
35	Suggested solution must have special detected category to block the website banners.	Kaspersky solution must have special detected category to block the website banners.	Suggested solution have special detected category to block the website banners.
36	Suggested solution must have ability to configure Wifi networks based on Network Name, Authentication Type, Encryption Type, that can later be used to block or allow the Wifi connections.	Kaspersky solution must have ability to configure Wifi networks based on Network Name, Authentication Type, Encryption Type, that can later be used to block or allow the Wifi connections.	Suggested solution have ability to configure Wifi networks based on Network Name, Authentication Type, Encryption Type, that can later be used to block or allow the Wifi connections.
37	User-based policies for device, web and application control	User-based policies for device, web and application control	User-based policies for device, web and application control
38	Suggested solution should allow blocking following devices: a) Bluetooth b) Mobile devices c) External modems d) CD/DVDs e) Transferring data to mobile device f) Camera and Scanners	Kaspersky solution should allow blocking following devices: a) Bluetooth b) Mobile devices c) External modems d) CD/DVDs e) Transferring data to mobile device f) Camera and Scanners	Suggested solution should allow blocking following devices: a) Bluetooth b) Mobile devices c) External modems d) CD/DVDs e) Transferring data to mobile device f) Camera and Scanners

Sl No.	Specifications	Firms	
		1	2
		M/s egs (PVT.) Ltd.	App in Snap (PVT.) Ltd.
39	Suggested solution should contain cloud integration for most up to date updates on malware and potential threats	Kaspersky solution should contain cloud integration for most up to date updates on malware and potential threats	Suggested solution contain cloud integration for most up to date updates on malware and potential threats
40	Suggested solution must have ability to manage user access rights for read and write operations on CDs/DVDs	Kaspersky solution must have ability to manage user access rights for read and write operations on CDs/DVDs	Suggested solution have ability to manage user access rights for read and write operations on CDs/DVDs
41	Suggested solution must have firewall filtering by local address, physical interface, and packet time-to-live (TTL).	Kaspersky solution must have firewall filtering by local address, physical interface, and packet time-to-live (TTL).	Suggested solution have firewall filtering by local address, physical interface, and packet time-to-live (TTL).
42	Suggest solution must allow administrator to enlist and monitor the application that use custom/random ports when launched.	Kaspersky solution must allow administrator to enlist and monitor the application that use custom/random ports when launched.	Suggest solution allow administrator to enlist and monitor the application that use custom/random ports when launched.
43	Suggested solution must support blocking blacklisted applications from being launched on endpoints. Also it must support blocking all applications except “whitelisted” ones	Kaspersky solution must support blocking blacklisted applications from being launched on endpoints. Also it must support blocking all applications except “whitelisted” ones	Support blocking blacklisted applications from being launched on endpoints. Also it must support blocking all applications except “whitelisted” ones
44	Suggested solution must have cloud-integrated application control component to get latest updates on applications’ rating and categories	Kaspersky solution must have cloud-integrated application control component to get latest updates on applications’ rating and categories	Have cloud-integrated application control component to get latest updates on applications’ rating and categories
45	Suggested solution must have ability to whitelist application based on the digital signature certificate, MD5, SHA256, META Data, File Path, Pre-defined security categories.	Kaspersky solution must have ability to whitelist application based on the digital signature certificate, MD5, SHA256, META Data, File Path, Pre-defined security categories.	Ability to whitelist application based on the digital signature certificate, MD5, SHA256, META Data, File Path, Pre-defined security categories.
46	Suggested solution must have controls for downloads of DLL and Drivers.	Kaspersky solution must have controls for downloads of DLL and Drivers.	Solution have controls for downloads of DLL and Drivers.
47	Suggested solution application control must have black list and white list operation modes	Kaspersky solution application control must have black list and white list operation modes	Suggested solution application control must have black list and white list operation modes
48	Suggested solution must support startup control of scripts from powershell	Kaspersky solution must support startup control of scripts from powershell	Support startup control of scripts from powershell
49	Suggested solution must support Test mode with report generation on launch of blocked applications	Kaspersky solution must support Test mode with report generation on launch of blocked applications	Support Test mode with report generation on launch of blocked applications
50	Suggested solution must have ability that restrict application activities within the system according to the trust level assigned to the application and limits the rights of applications to access certain resources, including system and user files.	Kaspersky solution must have ability that restrict application activities within the system according to the trust level assigned to the application and limits the rights of applications to access certain resources, including system and user files.	Provides ability that restrict application activities within the system according to the trust level assigned to the application and limits the rights of applications to access certain resources, including system and user files.
51	Suggest solution must have ability to control the system/user applications access to the Audio and Video recording devices.	Kaspersky solution must have ability to control the system/user applications access to the Audio and Video recording devices.	Have ability to control the system/user applications access to the Audio and Video recording devices.
52	Suggested solution must provide a facility to check applications listed in each cloud-based category	Kaspersky solution must provide a facility to check applications listed in each cloud-based category	Provide a facility to check applications listed in each cloud-based category
53	Suggested solution must have ability to integrate with Vendor Specific Advance Threat Protection system.	Kaspersky solution must have ability to integrate with Vendor Specific Advance Threat Protection system.	Have ability to integrate with Vendor Specific Advance Threat Protection system.
54	Solution must have ability to automatically regulate the activity of the running programs, access to the file system and registry as well as interaction with other programs	Kaspersky solution must have ability to automatically regulate the activity of the running programs, access to the file system and registry as well as interaction with other programs	Have ability to automatically regulate the activity of the running programs, access to the file system and registry as well as interaction with other programs
55	Solution must have the ability to automatically delete application control rules for the application if not launched from a specified interval. The interval must be configurable.	Kaspersky Solution must have the ability to automatically delete application control rules for the application if not launched from a specified interval. The interval must be configurable.	Have the ability to automatically delete application control rules for the application if not launched from a specified interval. The interval must be configurable.
56	Suggested solution must have the ability to automatically categorize the applications launched before/prior to the Endpoint protection installation	Kaspersky solution must have the ability to automatically categorize the applications launched before/prior to the Endpoint protection installation	Have the ability to automatically categorize the applications launched before/prior to the Endpoint protection installation

Sl No.	Specifications	Firms	
		1	2
		M/s egs (PVT.) Ltd.	App in Snap (PVT.) Ltd.
57	Suggested solution must have endpoint mail antivirus protection with; a) Attachment filter and ability to rename attachments b) Scan of mail messages when receiving, reading and sending	Kaspersky suggested solution must have endpoint mail antivirus protection with; a) Attachment filter and ability to rename attachments b) Scan of mail messages when receiving, reading and sending	Support endpoint mail antivirus protection with; a) Attachment filter and ability to rename attachments b) Scan of mail messages when receiving, reading and sending
58	Suggest solution must have ability to scan multiple redirects, shortened URLs, hijacked URLs, and time-based delays	Kaspersky Suggest solution must have ability to scan multiple redirects, shortened URLs, hijacked URLs, and time-based delays	Have ability to scan multiple redirects, shortened URLs, hijacked URLs, and time-based delays
59	Suggest solution must provide ability to the end user/user of the computer to perform check on the file reputation from the file context menu.	Kaspersky solution must provide ability to the end user/user of the computer to perform check on the file reputation from the file context menu.	Provide ability to the end user/user of the computer to perform check on the file reputation from the file context menu.
60	Suggested solution must include Scanning of scripts – scanning of all scripts, developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.), launched when the user works on the computer, including the Internet.	Kaspersky solution must include Scanning of scripts – scanning of all scripts, developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.), launched when the user works on the computer, including the Internet.	Include Scanning of scripts – scanning of all scripts, developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.), launched when the user works on the computer, including the Internet.
61	Protection against still unknown malware based of an analysis of their behavior and examination of changes in the system register, with the option of automatic restoration of system register values changed by the malware.	Protection against still unknown malware based of an analysis of their behavior and examination of changes in the system register, with the option of automatic restoration of system register values changed by the malware.	Protection against still unknown malware based of an analysis of their behavior and examination of changes in the system register, with the option of automatic restoration of system register values changed by the malware.
62	Protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type, including wireless networks.	Protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type, including wireless networks.	Protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type, including wireless networks.
63	IPv6 protocol support.	IPv6 protocol support.	IPv6 protocol support.
64	Special task for detecting vulnerabilities, with results available in reports	Special task for detecting vulnerabilities, with results available in reports	Special task for detecting vulnerabilities, with results available in reports
65	Scanning of critical sections of the computer as a standalone task.	Scanning of critical sections of the computer as a standalone task.	Scanning of critical sections of the computer as a standalone task.
66	Application self-protection technology, protection from unauthorized remote management of an application service as well as protection of access to application parameters via password, preventing the disabling of protection from malware, criminals or amateur users	Application self-protection technology, protection from unauthorized remote management of an application service as well as protection of access to application parameters via password, preventing the disabling of protection from malware, criminals or amateur users	Application self-protection technology, protection from unauthorized remote management of an application service as well as protection of access to application parameters via password, preventing the disabling of protection from malware, criminals or amateur users
67	Ability to choose which antivirus components will be installed.	Ability to choose which antivirus components will be installed.	Ability to choose which antivirus components will be installed.
68	Antivirus checking and disinfection of files packed using program like PKLITE, LZEXE, DIET, EXEPACK, etc.	Kaspersky Antivirus checking and disinfection of files packed using program like PKLITE, LZEXE, DIET, EXEPACK, etc.	Antivirus checking and disinfection of files packed using program like PKLITE, LZEXE, DIET, EXEPACK, etc.
69	Antivirus checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files.	Kaspersky Antivirus checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files.	Antivirus checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files.
70	Protection against still unknown malware belonging to registered families, based on heuristic analysis.	Protection against still unknown malware belonging to registered families, based on heuristic analysis.	Protection against still unknown malware belonging to registered families, based on heuristic analysis.

Sl No.	Specifications	Firms	
		1	2
		M/s egs (PVT.) Ltd.	App in Snap (PVT.) Ltd.
71	Availability of multiple ways to notify administrator about important events that have taken place (mail notification, audible announcement, pop-up window, log entry).	Availability of multiple ways to notify administrator about important events that have taken place (mail notification, audible announcement, pop-up window, log entry).	Availability of multiple ways to notify administrator about important events that have taken place (mail notification, audible announcement, pop-up window, log entry).
72	Suggested solution must allow the administrator to create a single installer with required configuration to non-IT literate users.	Kaspersky solution must allow the administrator to create a single installer with required configuration to non-IT literate users.	Allow the administrator to creat a single installer with required configuration to non-IT litrate users.
73	License for 03 years with regular updates through downloading of patch file/updates	License for 03 years with regular updates through downloading of patch file/updates	APP IN SNAP Provide License for 03 years with regular updates through downloading of patch file/updates
74	Installation, configuration with the existing system, and training of staff	Installation, configuration with the existing system, and training of staff	APP IN SNAP Provide Instalation, configuration with the existing system, and training of staff
75	Technical support for 01 year	Technical support for 01 year	APP IN SNAP Provide Technical support for 01 year
76	Dealership: Authorized Dealership with OEM certification	Dealership: Authorized Dealership with OEM certification	Yes Certificate Attached

Comments:

1 Two firms M/s egs (Pvt) Ltd. and M/s App in Snap (Pvt) Ltd. Islamabad have qouted technical specification for Antivirus.

2 M/s egs (Pvt) Ltd has replicated/copied technical specifications given in the tender, which reflects that the firm has failed to give proper technical quotes.

Recommendations:

Therefore, M/s App in Snap (Pvt) Ltd, Islamabad fulfils technical specifications and is recommeded for further proceedings, please.

TECHNICAL EVALUATION OF LED

Sl No.	Peripherals	Specifications	Firms	
			1	2
			M/s egs (PVT.) Ltd.	Paper Communication (PVT.) Ltd.
1	Brand	Panasonic/Sony/Samsung or equivalent	Samsung (Original) 50" 50BU8000 TV	Samsung
2	Series	5 Series	8 Series	7 Series
3	Type	LED TV	LED TV	LED TV
4	Screen Type	Flat Screen	Flat Screen	Flat Screen
5	Design	One Design (High Glossy)	AirSlim	Crystal UHD
6	Bezel Width	0.5" Thin	3 Bezel-less	3 Bezel-less
7	Stand Type (Color)	Square	Square	FLAT LIFT/black
8	Screen Size	49.5" Measured Diagonally	49.5" Measured Diagonally	49.5"
9	Resolution	1920 x 1080	3840 x 2160	3840 x 2160
10	Motion Rate*	60*Motion Rate replaces Clear Motion Rate as the Samsung measure of motion clarity	50Hz Motion Rate replaces Clear Motion Rate as the Samsung measure of motion clarity	
11	Dolby	Dolby Digital Plus / Dolby Pulse	Dolby Digital Plus / Dolby Pulse	OTS Lite
12	Sound Effect	SRS Theater Sound HD	SRS Theater Sound HD	Adaptive Sound
13	DTS Premium Sound	DTS 2.0 + Digital Out	Adaptive Sound	OTS Lite
14	Sound Output (RMS)	10W x 2	20W	2CH/20W
15	Speaker Type	Down Firing + Full Range	Down Firing + Full Range	2CH
16	Connect Share™	Movie	Movie	Connect Share™
17	OSD Language	English, Spanish, French	English, Spanish, French	Voice Guide: UK English, France French, Hindi, Russian, Korean OSD Language: Local Languages
18	Accessories	Closed Captioning, Game Mode, Eco Sensor, Auto Power Off, Clock & On/Off Timer	Closed Captioning, Game Mode, Eco Sensor, Auto Power Off, Clock & On/Off Timer	Eco Sensor, Auto Power off, Auto Game Mode
19	HDMI	2	3	3
20	USB	1	2	1
21	Component	1	1	no
22	Composite In (AV)	1 (Common Use for Component Y)	1 (Common Use for Component Y)	1 (Common Use for Component Y)
23	RF In (Terrestrial/Cable In put)	1	1	1
24	Digital Audio Out (Optical)	1	1	1
25	Audio Out (Mini Jack)	1	1	no
26	RS232C	Yes	Yes	no

Sl No.	Peripherals	Specifications	Firms	
			1	2
			M/s egs (PVT.) Ltd.	Paper Communication (PVT.) Ltd.
27	Digital Broadcasting	ATSC / Clear QAM	ATSC / Clear QAM	DVB-T2CS2
28	Power Supply (V)	ACI 10-240V 60Hz	ACI 10-240V 60Hz	ACI 10-240V 60Hz
29	Remote	Standard Remote Control (TM 1240)	Standard Remote Control (TM 1240)	TM2240A
30	Stand	Mini Wall Mount Compatibility	Mini Wall Mount Compatibility	Mini Wall Mount Compatibility
31	Vesa Wall Mount Compatibility	Yes (200 x 200)	Yes (200 x 200)	Vesa Wall Mount Support
32	Power Cable	Yes	Yes	Yes
33	User Manual	Yes	Yes	Yes
34	Warranty	01 years on site comprehensive	01 years on site comprehensive	01 years on site comprehensive

Comments:

1 Two firms M/s egs (Pvt) Ltd. and M/s Paper Communication (Pvt.) Ltd. Ibd. Quoted technical specifications for LED 50 INCH.

2 M/s egs (Pvt) Ltd. and M/s Paper Communication (Pvt.) Ltd both fulfill technical specifications.

Recommendations:

Therefore, M/s egs (Pvt) Ltd. and M/s Paper Communication (Pvt.) Ltd are recommended for further proceedings, please.

TECHNICAL EVALUATION OF FIREWALL

Sl No.	Peripherals	Specifications	Firms 1 App in Snap (PVT.) Ltd.
1	Brand	Renowned brand	**Huawei**
2	Basic Firewall	The appliance-based security platform should be a stateful NGFW, Next-Generation IPS, malware protection, URL protection, firewall, application visibility, and IPS functionality in a single appliance.	Physical/Hardware Appliance-based security platform should be a stateful NGFW, Next-Generation IPS, malware protection, URL protection, firewall, application visibility, and IPS functionality in a single appliance.
3	Hardware architecture	8×GE COMBO + 4×GE RJ45 + 4×GE SFP + 6×10GE SFP+ Single AC power supply; optional dual AC power supplies Optional, SATA (1×2.5 inch) supported, 240 GB/ 1TB	8×GE COMBO + 4×GE RJ45 + 4×GE SFP + 6×10GE SFP+ Single AC power supply; optional dual AC power supplies Optional, SATA (1×2.5 inch) supported, 240 GB/ 1TB
4	Performance requirements	Layer 3 throughput ⩾25Gbps; concurrent connections per second ≥ 10,000,000; new connections per second ≥250,000; IPSec VPN throughput (AES-256,1420 byte)≥25 Gbps Application controlling and IPS throughput ≥ 10 Gbps;	Layer 3 throughput ⩾25Gbps; concurrent connections per second ≥ 10,000,000; new connections per second ≥250,000; IPSec VPN throughput (AES-256,1420 byte)≥25 Gbps Application controlling and IPS throughput ≥ 10 Gbps;
5	Routing	Supports static routes, policy-based routing, and routing protocols such as RIP, OSPF, BGP, and IS-IS; Policy-based routing supports the following matching conditions: source IP address, destination IP address, service type, application type, user/user group/security group, inbound interface, and DSCP priority.	Supports static routes, policy-based routing, and routing protocols such as RIP, OSPF, BGP, and IS-IS; Policy-based routing supports the following matching conditions: source IP address, destination IP address, service type, application type, user/user group/security group, inbound interface, and DSCP priority.
6	Intelligent uplink selection	Supports service-specific PBR and intelligent uplink selection based on multiple load balancing algorithms (for example, based on bandwidth ratio and link health status) in multi-egress scenarios.	Supports service-specific PBR and intelligent uplink selection based on multiple load balancing algorithms (for example, based on bandwidth ratio and link health status) in multi-egress scenarios.

Sl No.	Peripherals	Specifications	Firms 1 App in Snap (PVT.) Ltd.
7	NAT	Supports full NAT functions and NAT ALG for multiple application-layer protocols, including ILS, DNS, PPTP, SIP, FTP, ICQ, RTSP, MSN, and MMS. Supports Source NAT automatic detection and exclusion of invalid addresses in NAT address pools. Firewall should support NAT444, NAT66 (IPv6-to-IPv6) , Nat46 (IPv4-to-IPv6) and DS-Lite NAT	Supports full NAT functions and NAT ALG for multiple application-layer protocols, including ILS, DNS, PPTP, SIP, FTP, ICQ, RTSP, MSN, and MMS. Supports Source NAT automatic detection and exclusion of invalid addresses in NAT address pools. Firewall should support NAT444, NAT66 (IPv6-to-IPv6) , Nat46 (IPv4-to-IPv6) and DS-Lite NAT
8	Traffic control	Supports application-layer protocol-based traffic control policies, including setting the maximum bandwidth, guaranteed bandwidth, and protocol traffic priority. Supports bandwidth guarantee based on users and IP addresses. Supports maximum number of connections per IP address.	Supports application-layer protocol-based traffic control policies, including setting the maximum bandwidth, guaranteed bandwidth, and protocol traffic priority. Supports bandwidth guarantee based on users and IP addresses. Supports maximum number of connections per IP address.
9	Intrusion prevention and antivirus	Supports attack detection and prevention based on over 7000 local signatures. Supports the customization of intrusion prevention policy templates based on scenarios. Supports brute-force cracking prevention for common application services (HTTP, FTP, SSH, SMTP, and IMAP) and database software (MySQL, Oracle, and MSSQL). Supports malicious domain name-based filtering to block C&C. Supports antivirus for protocols such as HTTP, FTP, SMTP, POP3, IMAP, and NFS.	Supports attack detection and prevention based on over 7000 local signatures. Supports the customization of intrusion prevention policy templates based on scenarios. Supports brute-force cracking prevention for common application services (HTTP, FTP, SSH, SMTP, and IMAP) and database software (MySQL, Oracle, and MSSQL). Supports malicious domain name-based filtering to block C&C. Supports antivirus for protocols such as HTTP, FTP, SMTP, POP3, IMAP, and NFS.

Sl No.	Peripherals	Specifications	Firms 1 App in Snap (PVT.) Ltd.
10	URL filtering	Provides a URL category database with over 120 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites. Supports DNS filtering, in which accessed web pages are filtered based on domain names. Supports the Safe Search function to filter resources of search engines, such as Google, to guarantee access to only healthy network resources.	Provides a URL category database with over 120 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites. Supports DNS filtering, in which accessed web pages are filtered based on domain names. Supports the Safe Search function to filter resources of search engines, such as Google, to guarantee access to only healthy network resources.
13	DDoS defense	Supports application-layer flood attacks such as HTTP, HTTPS, DNS, and SIP, supports traffic auto-learning, the setting of the auto-learning time, and automatic generation of anti-DDoS policies.	Supports application-layer flood attacks such as HTTP, HTTPS, DNS, and SIP, supports traffic auto-learning, the setting of the auto-learning time, and automatic generation of anti-DDoS policies.
14	Policy & Management	Allows users to configure security policies based on time, application-layer protocol, geographical location, IP address, port, domain name group, URL category, access type, vlanID and content security.	Allows users to configure security policies based on time, application-layer protocol, geographical location, IP address, port, domain name group, URL category, access type, vlanID and content security.
15	Network access user authentication	Supports multiple user authentication methods, including local, RADIUS, HWTACACS, AD, and LDAP.	Supports multiple user authentication methods, including local, RADIUS, HWTACACS, AD, and LDAP.
16	License	Provides the related Full threats protection License of 03 Years	Yes provides the related Full threats protection License of 03 Years
17	Reliability	Supports BFD link detection and association of BFD and VRRP/OSPF to implement rapid active/standby switchover. Supports the smooth upgrade of HA(Active/Active or Active/Standby) Mode, the software of different versions can be used for hot standby.	Supports BFD link detection and association of BFD and VRRP/OSPF to implement rapid active/standby switchover. Supports the smooth upgrade of HA(Active/Active or Active/Standby) Mode, the software of different versions can be used for hot standby.
18	Product certification	Has been listed as Leader or Challenger in Gartner Magic Quadrant;	Listed as a Challenger in Gartner Magic Quadrant;

Sl No.	Peripherals	Specifications	Firms 1 App in Snap (PVT.) Ltd.
19	Warranty Service	3 years licenses and hardware support should be a part of proposal	3 years licenses and hardware support should be a part of proposal
20	Dealership	Authorized Dealership certification of OEM	Authorized Dealership certification Attached

Comments:

1 Only one firm, M/S App in Snap (Pvt) Ltd., Islamabad, participated in technical specifications for Firewall.

2 M/S App in Snap (Pvt) Ltd. Islamabad, fulfils tender specifications.

Recommendations:

Therefore, M/s App in Snap (Pvt) Ltd. Islamabad is recommended for further proceedings, please.