Jadual 1

# JADUAL PEMATUHAN TEKNIKAL

**SEBUTHARGA PEMBAHARUAN 2500 UNIT LESEN PERISIAN ANTIVIRUS KASPERSKY DAN TERMASUK PENYELENGGARAAN (PEMBAIKAN & PENCEGAHAN) BAGI PERISIAN DAN SEPULUH (10) UNIT SERVER ANTIVIRUS KASPERSKY BAGI TEMPOH SATU (1) TAHUN UNTUK KEGUNAAN PEJABAT SETIAUSAHA KERAJAAN NEGERI SELANGOR DAN SEMBILAN (9) PEJABAT DAERAH DAN TANAH SELANGOR**

**i) SPESIFIKASI PERISIAN ANTIVIRUS UNTUK PERLINDUNGAN BAGI WORKSTATION, LAPTOPS, SMARTPHONE DAN SERVER DALAM RANGKAIAN PEJABAT SUK SELANGOR (MINIMUM REQUIREMENTS)**

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | Antivirus Software to protect Workstation, Laptops, Smart Phone, File Servers and Networked Storage on the network with the following functionality: | 2500 Unit | | |
| 1. | Brand and Product : Antivirus Kaspersky Endpoint Business Select **(Latest version)** | | | |
| | i. desktops | | | |
| | ii. smartphone | | | |
| | iii. servers | | | |
| 2. | Shall provide support for centralized management and policy based antivirus configuration | | | |
| 3. | Shall support the following platform | | | |
| | i. Microsoft Windows<br>• Windows Workstation XP/Vista/Windows7, 8, 10<br>• Windows Server 2003/2008/2012 | | | |
| | ii. Macintosh OS | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | iii. Mobile OS (Windows Mobile, Android & iOS) | | | |
| | iv. Linux OS<br>• Redhat, CentOS, Fedora, SUSE Linux, Novell Open Entterprise, OpenSUSE Linux, Debian GNU, Mandriva, Ubuntu, Linux XP Enterprise Desktop, FreeBSD | | | |
| | v. Novell Netware | | | |
| 4. | Shall provide continuous virus protection by providing real time protection scanning (Hybrid technology - using both signature and cloud assisted scanning engine) | | | |
| 5. | Shall provide on demand anti-virus scanning (Hybrid technology - using both signature and cloud assisted scanning engine) | | | |
| 6. | Shall be able to scan | | | |
| | i. 1,200 types of compression archive formats or versions | | | |
| | i. with unlimited layers of compression by different archivers | | | |
| | ii. Include recursive scanning (for example a zip within a zip within a RAR) | | | |
| | ii. Include protection against “archive bombs” | | | |
| | iii. Compressed with GZIP | | | |
| 7. | Shall automatically clean viruses in most commonly used archive files | | | |
| | i. ZIP, ARJ, CAB, LHA, RAR, TAR | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | i. with unlimited layers of compression | | | |
| 8. | Shall be able to scan more than 2000 version of executable packers | | | |
| 9. | Shall protect from all types of malicious programs including viruses, ad ware, spy ware, dialers, trojans and rootkit within one fully functional standard product | | | |
| 10. | Must integrate with KSN cloud assisted technology for getting information on file and URL reputation<br>i) A KSN proxy is provided to reduce network traffic and provide faster response<br>ii) With over 3 billion files in the reputation database<br>iii) With more than 300 million unique clean files<br>iv) Globally deployed cloud infrastructure that integrates a network of at least 300 million customers | | | |
| 11. | Must provide the following reputation services<br>i) Application activity monitor: Reputation<br>ii) Monitoring running applications (even trusted one)<br>iii) Grouping applications based on trustworthiness, evaluation across the following sources<br>a. Signature bases<br>b. Analytical protection modules<br>c. Cloud<br>i. Trusted programs<br>ii. Trusted websites<br>iii. Suspicious program<br>iv. Suspicious websites<br>iv) Urgent detection system | | | |
| 12. | Shall scan incoming and outgoing e-mail messages of any mail clients that use SMTP, IMAP, MAPI, NNTP and POP3 protocols | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| 13. | Native integration with MS Outlook, The Bat!, Microsoft Outlook Express, Windows Mail and Mozilla Thunderbird. | | | |
| 14. | Shall support deployment by the following mechanisms: | | | |
| | i. Any corporate management solution that support Microsoft Installer (MSI) | | | |
| | i. Log-in script | | | |
| | ii. Client Package | | | |
| | iii. Windows Domain Group Policy | | | |
| | iv. Push Method | | | |
| | v. Active Directory | | | |
| 15. | Shall provide real-time lock down of client configuration – allow or prevent users from changing settings or unloading/uninstalling the software | | | |
| 16. | Shall provide password protection to prevent AV software from being uninstalled by end users (even with Administrator privileges) | | | |
| 17. | Shall be able to perform updates regardless of whether the client is connected to the management server | | | |
| | Shall support the following update propagation sources | | | |
| | i. Administration Server (push & pull) | | | |
| | i. Network Shares (SMB protocol) | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | ii. HTTP and FTP sites | | | |
| | iii. The antivirus manufacturer's site | | | |
| 18. | Shall provide the following protection to workstations | | | |
| | i. File anti-virus : with iSwift and iChecker technology | | | |
| | i. Mail anti-virus | | | |
| | ii. Web anti-virus | | | |
| | iii. IM Anti-virus | | | |
| | iv. System watcher | | | |
| | v. Network Attack Blocker | | | |
| | vi. Application control | | | |
| | vii. Registry protection | | | |
| | viii. Anti-banner | | | |
| | ix. Anti-dialer | | | |
| | x. Firewall | | | |
| | xi. IDS | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | xii. External device control (example, disable USB thumb drive, disable modem/broadband) | | | |
| 19. | Must provide the following application control function | | | |
| | i. Integrated with vendor cloud service | | | |
| | i. Application startup control | | | |
| | ii. Application privilege control | | | |
| | iii. Golden category – with known trusted applications updated by vendor | | | |
| | iv. Possibility to apply to particular groups of users/computers | | | |
| | v. Possibility to restrict some particular actions for specified applications/groups (device access, registry access, self copying, spawning own processes etc) | | | |
| | vi. Provide software inventory<br>a. Network wide application inventory<br>b. Company wide application inventory | | | |
| | vii. Test rules | | | |
| | viii. Cloud based object reputation | | | |
| | ix. Application trust elevation (user is able to send request to administrator via interface) | | | |
| | x. Ability to restrict vulnerable application | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | xi. Provide categorization<br>c. Provide about 100 defined categories<br>d. At least 300 million known good files | | | |
| | i. Integration with AD/LDAP | | | |
| | i. Provide the following blacklisting<br>e. Blacklisting applications<br>f. Blacklisting groups<br>g. Blacklisting categories<br>h. Blacklisting by Security rating | | | |
| 20. | Shall be able to perform damage cleanup of Trojans and worms | | | |
| 21. | The anti-virus engine | | | |
| | i. Shall use single scanning agent | | | |
| | i. Shall not require opening port at host level for updates | | | |
| | ii. Shall be able to detect all types of viruses (Trojan/Worm, joke, Hoax, Dialer etc) | | | |
| | iii. Shall be able to scan only file types which are potential virus carriers (based on true file type) | | | |
| | iv. Shall be able to cure infected files, quarantine suspicious files | | | |
| 22. | Shall support list of trusted application / processes | | | |
| 23. | Shall be able to restrict some particular actions for specified applications/groups (device access, registry access, self-copying, spawning own processes etc.) | | | |
| 24. | Shall support on-demand antivirus scanning launch using command line with customizable parameters | | | |

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| 25. | Shall provide Smart Phone protection | | | |
| | i. Shall support the following platform | | | |
| | a) Windows Mobile 8.1, 10 | | | |
| | b) Android 4.0 – 6.0 | | | |
| | c) iOS 7.0 – 9.0 | | | |
| | ii. Shall provide the following function | | | |
| | a) Can be deployed and managed by administration server | | | |
| | a) Anti-virus | | | |
| | b) Encryption | | | |
| | c) Firewall | | | |
| | d) Privacy protection | | | |
| | e) Anti-theft | | | |
| | - Remotely lock mobile device | | | |
| | - Remotely wipe mobile device | | | |
| | - Remotely locate mobile device using GPS | | | |
| | f) SIM-Watch | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| 26. | Shall provide frequent database update, with at least 10 updates per day (average) | | | |
| 27. | Shall be able to hide the presence of Anti-virus software on user machines (on Microsoft Windows platform) | | | |
| 28. | Must provide the following application control function | | | |
| | i. Integrated with vendor cloud service | | | |
| | i. Application startup control | | | |
| | ii. Application privilege control | | | |
| | iii. Golden category – with known trusted applications updated by vendor | | | |
| | iv. Possibility to apply to particular groups of users/computers | | | |
| | v. Possibility to restrict some particular actions for specified applications/groups (device access, registry access, self copying, spawning own processes etc.) | | | |
| | vi. Provide software inventory<br>a) Network wide application inventory<br>b) Company wide application inventory | | | |
| | vii. Test Rules | | | |
| | viii. Cloud based object reputation | | | |
| | ix. Application trust elevation (user is able to send request to administrator via interface) | | | |

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | x. Ability to restrict vulnerable application | | | |
| | xi. Provide categorization<br>a) Provide about 100 defined categories<br>b) At least 300 million known good files | | | |
| | i. Integration with AD/LDAP | | | |
| | i. Provide the following blacklisting<br>a) Blacklisting applications<br>b) Blacklisting groups<br>c) Blacklisting categories<br>d) Blacklisting by Security rating | | | |
| 29. | Must provide the following reputation services | | | |
| | i. Application activity monitor: reputation | | | |
| | i. Monitoring running applications (even trusted one) | | | |
| | ii. Grouping applications based on trustworthiness, evaluation across the following sources;<br>a) Signature bases<br>b) Analytical protection modules<br>c) Cloud<br>(1) Trusted programs<br>(2) Trusted websites<br>(3) Suspicious program<br>(4) Suspicious websites | | | |
| | iii. Urgent detection system | | | |
| 30. | Must provide advanced Proactive technologies and heuristics as follows; | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | i. System Watcher | | | |
| | i. Behavior Streams Signature technology (updatable) | | | |
| 31. | Must provide the following Web controls and content filtering | | | |
| | i. Filtering of Web resources by URL, content and data type | | | |
| | i. Flexible controls to grant permission, prohibit, limit or conduct user audits for certain categories of websites | | | |
| | ii. Flexible scheduling of web usage rules enable web access during certain hours | | | |
| | iii. Integration with Active Directory | | | |
| | iv. Possibility to test new rules created before they are applied effectively | | | |
| | v. Reports detailing PC usage for web browsing | | | |
| 32. | Must integrate with KSN cloud for getting information on file and URL reputation | | | |
| | i. A KSN proxy is provided to reduce network traffic and provide faster response | | | |
| | i. With over 3 billion files in the reputation database | | | |
| | ii. (With more than 300 million unique clean files | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | iii. Globally deployed cloud infrastructure that integrates a network of at least 300 million customers | | | |
| 33. | Must support QScan technology. A deep scanning technology that works at the lowest levels of the operating syste to remove any malware detected at the root of a user's system | | | |
| 34. | Shall be able to view action against detected malware that has been quarantined and to do back-up storage before proceeding with remedial actions | | | |
| 35. | Shall provide scanning of ICQ/MSN/AIM traffic | | | |
| 36. | Shall analyze the behavior of all processes running in the system and saves all changes made in the file system and the registry | | | |
| 37. | Shall detects most implementation of existing root kits, which are capable of concealing files, folders and registry keys from the user, as well as hiding running programs, system services, drivers, network connection and network activities | | | |
| 38. | Shall detect phishing attacks | | | |
| | i. when receiving messages containing links to phishing sites | | | |
| | i. when opening web pages in the browser | | | |
| 39. | Shall support automated virus outbreak prevention on server platform | | | |
| 40. | Shall have protection from hacker attacks | | | |
| 41. | Shall have terminal server protection | | | |
| 42. | Shall be able to update signature databases for better detection of malicious files and lower signature update size | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | (a) signature based technology | | | |
| 43. | PROTECTION FROM KNOWN, UNKNOWN AND ADVANCED MALWARE on Corporate Server | | | |
| | The solution shall ensures faster scans and less impact on system resources, providing the highest detection rate supported by cloud-assisted security | | | |
| | The solution shall provide unprecedented security by using configured rules to allow or block the startup of executable files, scripts, and MSI packages, or the loading of DLL modules onto servers. | | | |
| | The solution shall protect shared folders from crypto-malware (Anti-Cryptor). The application blocks the originating machine from accessing any network file resources when file encryption activity is detected, | | | |
| | The solution shall block access from hosts with suspicious activity, blocks computer access to shared network folders on a protected server while running the Real-Time File Protection or Anti-Cryptor tasks. | | | |
| | The solution shall scan the operating system's critical areas. A dedicated task can be run to scan those areas of the operating system that are most exposed to infection. | | | |
| | Scope of flexible scan setting enable Administrator to :<br><br>i) Exempt certain processes from scanning<br>ii) Set the depth of protection<br>iii) Specify which file types must always be scanned and which should be exempted<br>iv) Pre-set responses to suspicious and infected objects according to threat type | | | |

Jadual 1

| BIL | SPESIFIKASI | KUANTITI | MEMATUH (YA/TIDAK) | CADANGAN PENYEBUTHARGA |
|---|---|---|---|---|
| | The solution shall allocate resources between Endpoint Server and other applications according to pre-assigned priorities: anti-malware scans can also run in background mode. | | | |
| | The solution shall able to select trusted processes from scanning for performance optimization purposes. | | | |
| | The solution shall able to prevent uninterrupted server operation such as reboot whenever anti-malware protection is installed or updated. | | | |
| | The solution shall support flexible administration over<br><br>i) Selection of management tools.<br>ii) Easy-to-use installation and management tools.<br>iii) Control over administrator privileges.<br>iv) Flexible setting of scan times.<br>Notification system. | | | |
| | The solution shall compatible with virtualization platforms and operational systems. | | | |

Jadual 1

**i) SOFTWARE SPECIFICATION FOR ENTERPRISE MANAGEMENT CONSOLE FUNCTIONALITY FOR CENTRALIZED VIRUS CONTROL (MINIMUM REQUIREMENTS)**

| BIL. | SPESIFIKASI | KUANTITI | MEMATUHI (YA/TIDAK) | CATATAN |
|---|---|---|---|---|
| | **Enterprise Management Console functionality for centralized virus control for automatic dissemination of the latest Anti-Virus Signatures across the Enterprise** | | | |
| 1. | Shall be able to manage the anti-virus programs on a local area network (LAN) from a single console | | | |
| 2. | Shall be able to manage anti-virus programs on wide area network (WAN) from a single console | | | |
| 3. | Shall be able to build a multiple layer of Administration server relationship for example Mother-child / Master-slave relationship, and support unlimited number of sub-level administration server | | | |
| 4. | Shall provide ability to limit data transfer rate between administration server during peak hours | | | |
| 5. | Shall be able to create and apply customized policy to multiple workstations on a logical network | | | |
| 6. | Shall allow the anti-virus administration server to remotely install anti-virus “at the background” without interrupting the target workstation activities | | | |
| 7. | Shall be able to manage quarantine and backup storage base on disk space size and day stored. Quarantine files are scanned after each update and backup can be stored to the original folder | | | |

Jadual 1

| BIL. | SPESIFIKASI | KUANTITI | MEMATUHI (YA/TIDAK) | CATATAN |
|---|---|---|---|---|
| 8. | Shall provide notification for Error, Warning, Critical and Info (E.g. License Key Expired, anti-virus database, updates missed, virus deleted, not scanned for a long period) | | | |
| 9. | Shall provide the following notification to administrator<br>(a) Email<br>(b) SNMP<br>(c) Netsend<br>(d) Event log | | | |
| 10. | Shall give limited access to workstation to change the anti-virus setting for security purpose | | | |
| 11. | Shall provide password to avoid user make any changes on the policy | | | |
| 12. | If the workstation failed to run at the scheduled time, it shall automatically update Anti-Virus database when Windows is launched in the future | | | |
| 13. | Shall be able to scan automatically when windows is start –up after it failed to run during the scheduled time | | | |
| 14. | Management console must provide both MCC compliance and Web interface | | | |
| 15. | Shall provide policy and tasks inheritance throughout the administration servers hierarchy | | | |
| 16. | Shall provide a possibility to lock client setting on a higher level of hierarchy, thus preventing them from being changed in the lower level policies | | | |

Jadual 1

| BIL. | SPESIFIKASI | KUANTITI | MEMATUHI (YA/TIDAK) | CATATAN |
|---|---|---|---|---|
| 17. | Shall be able to perform centralized update for anti-virus database and software update | | | |
| 18. | Shall enable the administration server at the branch to get anti-virus database updates and/or application updates from the Central Anti Virus server in the headquarters. If the Central Anti Virus server fails, it can get updates from the internet | | | |
| 19. | Shall support the following update propagation sources | | | |
| 20. | (a) Administration Server (push & pull) | | | |
| | (b) Update Agent | | | |
| | (c) Network Shares (SMB protocol) | | | |
| | (d) HTPP and FTP sites | | | |
| | (e) The anti-virus manufacturer's site | | | |
| 21. | Shall provide the function for automated database update testing on a model machine, before the database update are allowed to be distributed to managed machines | | | |
| 22. | Shall support deployment by the following mechanisms: | | | |
| | (a) Any corporate management solution that support Microsoft Installer (MSI) | | | |
| | (b) Log-in script | | | |
| | (c) Client Package | | | |
| | (d) Windows Domain Group Policy | | | |
| | (e) Push Method | | | |

Jadual 1

| BIL. | SPESIFIKASI | KUANTITI | MEMATUHI (YA/TIDAK) | CATATAN |
|---|---|---|---|---|
| | (f) Active Directory | | | |
| 23. | Shall provide the creation of modified installation package | | | |
| 24. | Shall provide the creation of installation package that include the latest database update | | | |
| 25. | Shall provide the ability to install third-party software through administration server | | | |
| 26. | Shall provide policy enforcement and updates propagation when the client is located behind a NAT or any Firewall that allows only client initiated connections | | | |
| 27. | Shall be able to monitor remote locations over WAN links for antivirus activity | | | |
| 28. | Shall provide incident monitoring and notification | | | |
| 29. | System reporting shall provide information collected throughout the network hierarchy for analysis of activity, graphical report generation (templates provided) | | | |
| 30. | Support centralized view and management of quarantined objects across the AV network from administration console | | | |
| 31. | Shall provide a mechanism for randomization of client task execution schedule in order to decrease number of simultaneous client requests to the administration server | | | |
| 32. | Shall have a mechanism for backup and Restore of Administration Server | | | |

Jadual 1

| BIL. | SPESIFIKASI | KUANTITI | MEMATUHI (YA/TIDAK) | CATATAN |
|---|---|---|---|---|
| 33. | Shall provide automatic virus attack detection with automatic activation of specific policy | | | |
| 34. | Shall be able to perform all necessary outbreak related tasks from a single interface | | | |
| 35. | Shall be able to have different operator assigned separate access to individual location for job delegation and separation of task and responsibility | | | |
| 36. | Shall support integration with Windows security subsystem for administrator/operator authentication | | | |
| 37. | Shall utilize SSL-encrypted communications between management server and managed product(s) | | | |
| 38. | Shall support customization of the virus signatures update interval | | | |
| 39. | Workstation can be categorized based on its critical condition such as “Critical status”, “Warning-need attention” and “Detection” of new workstation in the network | | | |
| 40. | Shall perform real-time information status of the anti virus on administration server | | | |
| | (a) Start and Stop anti-virus activity | | | |
| | (b) On demand scan and update | | | |
| | (c) Real time protection status | | | |
| | (d) Workstation system information | | | |
| 41. | Shall be able to control devices by: | | | |

Jadual 1

| BIL. | SPESIFIKASI | KUANTITI | MEMATUHI (YA/TIDAK) | CATATAN |
|---|---|---|---|---|
| | (a) Type of devices (Removable drive, printers, Portable devices etc) | | | |
| | (b) Device control on bus level (Infrared, Serial Port etc) | | | |
| | (c) Device control by trusted devices ( Device ID, Device Model) | | | |
| | (d) Default deny for devices | | | |
| | (e) Read/write permission granularity | | | |
| | (f) Integration with AD | | | |

**ii) KASPERSKY SERVER MANGEMENT INCLUSIVE PREVENTIVE AND CORRECTIVE MAINTENANCE**

| BIL. | SPESIFIKASI | MEMATUHI (YA/TIDAK) | CATATAN |
|---|---|---|---|
| | **Dell server Support Solution (One (1) Year Warranty Extension From Dell)** | | |
| 1 | Technical support access<br>- 24x7 | | |
| 2 | Part and labour response<br>- NBD or Mission Critical | | |
| 3 | TechDirect online cases and despatch | | |
| 4 | SupportAssist remote monitoring | | |
| 5 | Dispatch monitoring and crisis management | | |
| 6 | Escalation management | | |
| 7 | Hypervisor and OS support | | |
| 8 | SupportAssist automated support | | |
| 9 | Direct access to elite ProSupport Plus engineers | | |
| 10 | Dedicated Technical Account Manager | | |
| 11 | Health check and performance recommendations during Preventive Maintenance | | |
| 12 | System maintenance | | |

**iii) SKOP PERKHIDMATAN SOKONGAN**

| NO. | SKOP | PERKHIDMATAN MANDATORI (M) | CATATAN | MEMATUHI (YA/TIDAK) | CADANGAN PEYEBUTHARGA |
|---|---|---|---|---|---|
| 1. | Memperbaharui 2500 unit lesen antivirus Kaspersky di Pejabat SUK Selangor (Bangunan SSAAS), SPN (SUK 2) dan Sembilan (9) Pejabat Daerah dan Tanah Selangor | M | 8 jam x 5 hari seminggu | | |
| 2. | Software Coverage | M | 8 jam x 5 hari seminggu | | |
| 3. | Centralised Antivirus System | M | 8 jam x 5 hari seminggu | | |
| 4. | On-site technical Support | M | - 8 jam x 5 hari seminggu<br>- 55 jam setahun bagi aduan insiden di HQ SUK (Bangunan SSAAS & SPN) termasuk 9 Pejabat Daerah seluruh Selangor<br>- 5 insiden setahun di HQ SUK | | |

Jadual 1

| NO. | SKOP | PERKHIDMATAN MANDATORI (M) | CATATAN | MEMATUHI (YA/TIDAK) | CADANGAN PEYEBUTHARGA |
|---|---|---|---|---|---|
| | | | (Bangunan SSAAS & SPN) dan 9 Pejabat Daerah seluruh Selangor pada hari Sabtu dan Ahad | | |
| 5. | Preventive Maintenance (Perisian antivirus & Server) | M | 2 kali setahun di HQ SUK (Bangunan SSAAS & SPN) dan 9 Pejabat Daerah seluruh Selangor | | |
| 6. | On-Site Training (instalation, configuration and antivirus operation for Administrator) - 3 orang pentadbir | M | | | |
| 7. | Corrective Maintenance (Perisian antivirus, OS, alat ganti server, labour) | M | | | |
| 8. | Memastikan pelaksanaan antivirus adalah secara berpusat berjaya dan berfungsi dengan baik iaitu semua client mendapat update daripada server | M | | | |
| 9. | Memastikan *password* ditukar kepada yang baharu. (tertakluk kepada persetujuan Pej. SUK Selangor) | M | | | |

Jadual 1

| NO. | SKOP | PERKHIDMATAN MANDATORI (M) | CATATAN | MEMATUHI (YA/TIDAK) | CADANGAN PEYEBUTHARGA |
|---|---|---|---|---|---|
| 10. | Jaminan extended satu (1) tahun bagi server hendaklah diperolehi daripada pihak prinsipal server bagi memastikan alat ganti tulen dan dijamin oleh prinsipal. Sila lampirkan **surat Authorization DAN surat Extended Warranty** daripada principal; | M | | | |
| 11. | Tarikh atau bulan pembaharuan lesen Kaspersky dan extended warranty bagi server antivirus hendaklah sama supaya pemantauan dapat dibuat dengan lebih berkesan; | | | | |
| 12. | Penyelenggaraan pencegahan (PM) bagi 2500 pengguna lesen perisian antivirus dan sepuluh (10) unit sever antivirus sebanyak dua (2) kali setahun dan **laporan penuh** (bukan sekadar job sheet/checklist) hendaklah dikemukakan dalam tempoh empat belas (14) hari selepas kerja-kerja PM dijalankan; | M | | | |
| 13. | Melaksanakan pengujian ***backup and restore*** terhadap konfigurasi security center atau yang berkaitan dan database server antivirus di lokasi-lokasi yang telah dinyatakan di atas; | M | | | |
| 14. | Penyelenggaraan pembaikan dibuat oleh pihak syarikat yang dilantik oleh Kerajaan meliputi pembaikan perisian antivirus dan server; | M | | | |

Jadual 1

| NO. | SKOP | PERKHIDMATAN MANDATORI (M) | CATATAN | MEMATUHI (YA/TIDAK) | CADANGAN PEYEBUTHARGA |
|---|---|---|---|---|---|
| 15. | Penyelenggaraan pembaikan server hendaklah termasuk operating system (OS) bagi server dan kerja-kerja formatting server sekiranya diperlukan; | M | | | |
| 16. | Tindakbalas aduan hendaklah dalam masa 4 jam selepas aduan dibuat | M | | YA | |
| 17. | Pertukaran perkakasan setara atau loan unit hendaklah disediakan bagi perkakasan yang memerlukan masa untuk dibaiki dengan syarat dipersetujui oleh pegawai BTM; | M | | | |
| 18. | Pertukaran/penggantian part hendaklah dilakukan dalam masa Next Business Day (NBD) secara onsite; | M | | | |
| 19. | Pihak syarikat hendaklah datang ke lokasi aduan (onsite support) dibuat untuk mengambil perkakasan yang rosak dan mengembalikan semula selepas kerja-kerja pembaikan dibuat atau menggantikan dengan alat ganti yang baru dengan kos yang ditanggung oleh pihak syarikat; | M | | | |
| 20. | Semua kos penggantian spare part perkakasan server yang dinyatakan di dalam Jadual 1 adalah di bawah tanggungjawab pihak syarikat dan pihak Kerajaan Negeri Selangor tidak akan membayar kos pembaikan dan penghantaran yang terlibat sepanjang tempoh kontrak dan; | M | | | |

Jadual 1

| NO. | SKOP | PERKHIDMATAN MANDATORI (M) | CATATAN | MEMATUHI (YA/TIDAK) | CADANGAN PEYEBUTHARGA |
|---|---|---|---|---|---|
| | | | | | |
| 21. | Tempoh penyempurnaan pembaharuan lesen, pengujian dan pengesahan oleh pegawai BTM untuk keseluruhan 2500 unit lesen adalah selama **60 hari dari tarikh SST ditandatangan** (sila kemukakan Gantt Chart) | M | | | |
| 22. | Penyebutharga hendaklah bekerjasama dengan pihak principal Kaspersky untuk memaklumkan kepada Kerajaan Negeri Selangor sekiranya terdapat serangan malware/virus/ancaman baru yang merbahaya yang boleh mengancam keselamatan rangkaian dan perkakasan di Negeri Selangor. | | | | |

***Nota :*** *Sila ambil maklum bahawa tempoh keseluruhan kontrak adalah bagi tempoh* ***SATU (1) TAHUN.***