The Oriental Insurance Company Limited
External Firewall

S.No	Features	Compliance Yes/No	Remarks
	General Requirements		
1	Firewall and Integrated IPSEC VPN Applications should be ICSA Labs certified for ICSA 4.0, FIPS 140-2 certified		
2	The proposed solution should support unlimited users with no limitations in terms of licencing for users		
3	OEM must have successfully completed NSS Lab's NGFW Methodology v5.4 testing with a minimum exploit blocking rate of 95%.		
4	OEM Should have block rate of min 95% in NSS labs breach detection system methodology2.0 and a recommended rating in the same		
5	Firewall and Integrated IPSEC VPN Applications should be ICSA Labs certified for ICSA 4.0, FIPS 140-2 certified		
	Hardware and Interface Requirements		
6	The complete solution should be based on dedicated hardware Appliance.		
7	The platform must be supplied with at least 6 x 10/100/1000Mbps interfaces port.		
8	Should have RJ45/micro USB console port		
9	The appliance should have min 1 Console port and min 1 USB Ports		
10	Should be open architecture based on multicore CPU's to protect & scale against latest dynamic security threats. ASIC based solution is not acceptable		
11	The appliance should have inbuild storage of 320 GB		
	Performance Requirements for Solution		
12	The appliance support firewall stateful inspection throughput of min 4 Gbps (RFC) and min 2.1 Gbps in real world/enterprise mix conditions		
13	Firewall should support minimum 3M concurrent sessions		
14	Firewall should support minimum 48,000 connections per second		
15	The appliance support IPS throughput of 1.4 Gbps		
16	The appliance should provide a overall real world throughput (NGFW Throughput) of 1.1 Gbps		
	Architecture Features		
17	The appliance must have options for on field serviceability like addition of memory, HDD, interface cards, interfaces etc		
18	The appliance must have at least 1 spare slot for future expansion of cards like interface cards, ports, bypass cards etc		
19	Firewall, IPS & Application Control, all modules must support inspecting traffic in Active-Active mode with and without multicontext mode.		
20	The Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades		
	Firewall & VPN Requirements		
21	Network Security Firewall should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.		
22	Firewall should support at least 500 protocols		
23	The Firewall must provide state engine support for all common protocols of the TCP/IP stack		
24	The Firewall must provide NAT functionality, including dynamic and static NAT translations		

25	The solution should support the IPSec VPN for both Site-Site & Remote Access VPN		
26	Firewallsystem should support to provision Route-Based IPSec VPN		
27	IPSec encryption should be supported with 3DES, AES-128 & AES-256 standards		
28	The VPN solution should support client based VPN for IPSeC/SSL as well as client less SSL VPN funtionality both.		
29	Firewall should support authentication proxy for Remote VPN, HTTP/HTTPS Applications Access, and various other applications		
30	Firewall should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods		
31	Solution should support BGP, OSPF, RIPv1 &2, Multicast Tunnels, DVMRP protocols		
Application Control			
32	Solution should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports		
33	All internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes, Ms-Exchange etc		
34	It should support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP		
35	Application control database should contain more than 7000 applications including but not limited to Instant Messaging like Yahoo, MSN, ICQ, Skype (SSL and HTTP tunneled) , Peer-Peer applications, like Kazaa, Gnutella, Bit Torrent, IRC (over HTTP)		
36	The solution should support authentication protocols like LDAP, RADIUS and have support for local passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.		
37	QoS Support [Guaranteed bandwidth, Maximum bandwidth, Priority bandwidth utilization, QOS weighted priorities, QOS guarantees, QOS limits]		
38	Solution Should support Identity Access for Granular user, group and machine based visibility and policy enforcement		
IPS Feature Requirements			
39	IPS updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time		
40	The IPS should scan all parts of the session in both directions		
41	Should have flexibility to define newly downloaded protections will be set in Detect or Prevent mode.		
42	IPS Engine should support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behavior-based detection, Multi-element correlation.		
43	IPS profile can be defined to Deactivate protections with Severity, Confidence-level, Perormance impact, Protocaol Anomalies.		
44	IPS must provide option to deactivate all signature which have high impact on performance with a single click configurable option.		
45	Intrusion Prevention should have and option to add exceptions for network and services.		

46	Solution Must support to deactivate IPS automatically if Resource Utilization (CPU and Memory) reaches 90% and automatically activate IPS if same resource utilization comes down to 30%. Solution must also provide option to configure or modify these limits.		
47	IPS must have option to predefine action as detect and prevent for new signature downloaded in signature updates.		
48	IPS events/protection exclusion rules can be created and view packet data directly from log entries with RAW Packets and if required can be sent to Wireshark for the analysis.		
49	IPS should have the functionality of Geo Protection to Block the traffic country wise in incoming direction, outgoing direction or both. IPS also should alert through Mail if any IPS traffic/event detected from Specific Country.		
50	IPS should be able to detect and prevent imbeded threats with in SSL traffic.		
51	IPS shall be able to provide complete user visibility in the logs.		
	BOT Prevention/Anti Malware/Anti Virus Requirements		
52	Solution should be able to detect & Prevent bot outbreaks, Bot communication with C&C and APT attacks		
53	Solution should have an Multi tier engine to ie detect & Prevent Comand and Control IP/URL and DNS		
54	Solution should be able to detect & Prevent attack types ie, such as spam sending click fraud or self-distribution, that are associated with Bots		
55	Solution should be able to provide with Forensic tools which give details like Infected Users/Device,Malware type,Malware action etc		
56	Antivirus protection protocols for HTTP,HTTPS, CIFS, SSL etc		
57	The OEM malware update mechanism should include reputation, network signatures and suspicious email activity detection		
58	solution should have option to inspect/scan files coming from external, DMZ and All interfaces		
	Policy/Device Management		
59	Should provide dedicated hardware based centralized management for central configuration of features like FW, IPS, App Control, Anti virus/malware etc, provisioning, real-time monitoring, fault management, logging and customized reporting with the capability to create scheduled reports. Central Management Server should support configuration and presence in a management domain for up to minimum of 5 devices.		
60	Should support SNMP v2 & v3 traps, email alerts and SNTP/ NTP. Device should be able to send SNMP traps to centralized server and should provide login/ logout, configuration changes, dumps information.		
61	Should support sending of logs to centralized Syslog server.		
62	Solution must support web API for integration with home grown web application and it must support Json strings for web API requests, it should allow json scripts directly from firewall dashboard console.		

63	Management platform should be capable of integrating third party vulnerability information into threat policy adjustment routines and customized tuning work flows.		
64	Should support REST/XML based API to integrate with network management and monitoring systems.		
65	All devices and features should be accessible through single Management device console. Multiple devices for managing the solution will not be acceptable		
66	Solution must provide functionality to automatically save current state of configuration each time when any configuration changes in Security policy is enforced, and should have option to revert back to previous state stored state. It must be capable of storing atleast last 10 policies.		
67	Security Appliance must be able to accumulate multiple Operating System Images to boot from. While reverting OS to other preconfigured Image, configuration must not be lost.		
68	Management Server must allow administrator to choose to login in readonly or readwrite mode.		
Log Server, Reporting			
69	Log Server Must provide option to add exceptions for IPS on the fly from logs itself.		
70	Log Server must show all logs in single window.		
71	Log Server must use index files for fast access to log file contents		
72	Reporting Server Must have pre-defined report for various components of the securuity solution		
73	Solution must allow scheduling of reports daily, weekly and monthly with start and expiration date for reports to be generated automatically according to defined start and expiration dates		
74	Solution must send reports automatically via email to multiple email-ids in both HTML & PDF format		
Management, Reporting, Logging and Analysis			
75	Reproting solution should provide out of the box and customized reporting		
76	Reporting solution should provide graphical summary reports		
77	Any changes or commands issued by an authenticated user should be logged to a database.		
78	The solution must have Granular option to restrict various Administrator in Management server to view only limited set of Policy which they are meant to edit		
79	Management System should provide Event analysis, correlation and reporting.		
80	Management System should Quickly identify critical security events using dashboard, charts and maps		

	Internal Firewall - Must be from Diffrenet OEM of External Firewall		
S.No	**Features**	**Compliance (S/I/N)**	**Remarks**
Sr.No.	**UTM Specifications**	**Compliance Yes / No**	
1	**Firewall**		
2	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems		
3	The Proposed Firewall Vendor should be in the Leaders' Quadrant of Gartner Magic Quadrant for Unified Threat Management.		
4	Firewall appliance should have at least 8 x 10/100/1000 GE interfaces from day one and should be scalable to 16 GE ports in future.		
5	Firewall Throughput should be 5 Gbps		
6	Firewall should have 3DES IPSec throughput of 2 Gbps		
7	Firewall should support 2000 site-to-site VPN Tunnels.		
8	Firewall should support 30,000 new sessions per second		
9	Firewall should support 2 Million concurrent sessions		
10	The Firewall solution should support NAT64, DNS64 & DHCPv6		
11	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.		
12	The physical interface shall be capable of link aggregation, otherwise known as the IEEE 802.3ad standard, allows the grouping of interfaces into a larger bandwidth 'trunk'. It also allows for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk.		
13	The proposed system should have integrated Traffic Shaping		
14	The Firewall should have integrated SSL VPN solution to cater to 300 SSL VPN concurrent users.		
15	The Firewall & IPSEC VPN module shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification.		
16	The proposed system should support a) IPSEC VPN b) PPTP VPN c) L2TP VPN d) SSL VPN		
17	The device shall utilize inbuilt hardware VPN acceleration: a) IPSEC (DES, 3DES, AES) encryption/decryption b) SSL encryption/decryption		
18	The system shall support the following IPSEC VPN capabilities: a) Multi-zone VPN supports. b) IPSec, ESP security. c) Supports NAT traversal d) Supports Hub and Spoke architecture e) Supports Redundant gateway architecture		
19	The system shall support 2 forms of site-to-site VPN configurations: a) Route based IPSec tunnel b) Policy based IPSec tunnel		
20	The system shall support IPSEC site-to-site VPN and remote user		
21	The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.		
22	**Virtualization**		
23	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN) with minimum 10 Virtual Firewall license.		
24	**Intrusion Prevention System**		
25	The IPS capability shall minimally attain NSS Certification		
26	IPS throughput should be 1.5 Gbps		
27	The IPS detection methodologies shall consist of: a) Signature based detection using real time updated database b) Anomaly based detection that is based on thresholds		

28	The IPS should be able to inspect SSL sessions by decrypting the traffic.		
29	The IPS system shall have at least 3,000 signatures		
30	IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available		
31	In event if IPS should cease to function, it will fail open by default and is configurable. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved		
32	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.		
33	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending a alert and logging the incident		
34	Signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)		
35	**Threat Prevention**		
36	Firewall should have threat prevention throughput of 250 Mbps		
37	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services: a) HTTP, HTTPS b) SMTP, SMTPS c) POP3, POP3S d) IMAP, IMAPS e) FTP, FTPS		
38	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
39	**Application Control**		
40	The proposed system shall have the ability to detect, log and take action against network traffic based on over 2000 application signatures		
41	The application signatures shall be manual or automatically updated		
42	The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions		
43	**High Availability**		
44	The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component		
45	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.		
46	High Availability Configurations should support Active/Active or Active/ Passive		
47	The firewall VPN shall support the following PFS Diffie-Hellmann groups: 1 (768 bits), 2 (1024 bits), 5 (1536 bits), 14 (2048 bits), 19 (ECP 256 bits), 20 (ECP 384 bits), 21 (ECP 521 bits)		
48	The firewall VPN shall support for NAT-T and X-Auth		
Centralized Management			
49	The firewall management system shall be capable of managing up to 2000 NGFW nodes.		
50	The firewall shall provide simplify management of security policies by giving administrators the ability to create reusable network and service object groups that can be referenced by multiple security policies, simplifying initial policy definition and on-going policy maintenance.		
51	The firewall management system shall support hierarchical policy management such as policy template, inherit policy, sub-policies, also include policy snapshot to allow comparing or roll back of policies revision.		

52	The firewall management system must support creation of these type of the elements to be use/reuse in policies: Host (Single IP address), Network, Domain Names, Address Ranges, Zones, Groups (of different elements above)		
53	To simplify and re-use policies, the firewall must have the capability of creating Alias elements whereby a single element in a policy assigned on different Firewalls will interpret a different IP address or network.		
54	To simplify element definition, the firewall must be able to define elements using expressions to be used in rules.		
55	The firewall management system shall include option to define custom elements based on: Protocol, Ports or port range, Application or Service		
56	The firewall management system shall support “Drag & Drop” and “Type-in Search” of elements into the relevant policy fields to simplify policy creation.		
57	The firewall shall support the ability to control logging levels on a per Rule basis. The firewall shall support offline updating of content, firmware, or signature through the centralize firewall management system.		
58	The firewall management system shall support the ability to allow for Roll Back of upgrades and updates.		
59	The firewall management system shall provide 'Hit Counter' for rules during a defined period, to show how many times each rule in your Firewall Policy has matched actual network traffic		
60	The firewall management system shall support the ability to allow administrator to view/edit policies directly from audit / traffic log viewer, simplify policy refinement.		
61	The firewall management system shall support role-based access control (RBAC) and operation to limit access to control and limit administrators to specific functions within the firewall or its virtual contexts, allowing each administrator group to freely perform its tasks without affecting the other groups.		
62	The firewall management system shall provide graphic dashboard for display Firewall statistic such as: Engine Details, Application Usage, Inspection Overview, VPN Overview		
Logs Analysis			
63	The firewall shall offer centralized management with integrated log server, with options to upgrade to multi domain architecture.		
64	The logs displayed on the firewall management console shall minimally contain the following fields on the same page: Timestamp, Sender (which Firewall sends the log), Geo Location, Source and Destination IP, Source and destination port, Service / Application, User, NAT address / Interface, Client Executable/File/MD5 hash, Rule, Event description, hit counts, action		
65	The firewall management logging platform shall be able to display logs in real-time to aid faster troubleshooting and not having to manual refresh or auto-refresh at fixed intervals.		
66	The firewall management logging platform must be able to quickly filter to show relevant logs for analysis by means of drag and drop relevant fields into the filter column.		
67	The firewall management logging platform must be able to save custom filters so administrators can easily reused them on the next logs analysis. The firewall management logging platform shall provide visual representation of logs in charts or graphs for administrator’s analysis and ease of troubleshooting.		
68	The firewall management logging platform must be able to easily drilldown logs view to statistical view like charts and graphs and toggle back and fore between these views without needing to re-create the filtering again		

69	The firewall management logging platform must provide the option to save the drilled down view into a report directly to ease administrator's effort to recreate filters in reporting tool. The firewall management system shall include build-in incident case workflow system for forensic and investigation purpose.		
70	The firewalls management system shall support the option of exporting logs in CSV, XML, syslog and CEF and also capable of export into PDF and ZIP file. The firewall management system shall support real-time log forwarding in syslog, CEF, LEEF, XML, CSV, IPFIX and NetFlow formats.		
Alerts and Reporting			
71	The firewall management platform shall support the following alerting actions: SMS, SMTP (email), SNMP, Alert on Management Console, Run a custom script. The firewall shall support SNMPv1, v2c and v3		
72	The firewalls management system shall support the detection and notification of performance degradation such as critically high CPU and memory utilization and when maximum supported number of concurrent sessions reached.		
73	The firewall management platform shall allow for alert chaining which provides escalation of alerts based on severity and acknowledgement status. The firewall management platform must have the granularity to send different alert chains during different times, definable by Day and Time.		
74	The firewall management system must be able to define a threshold for alerts to prevent administrator's email from being flooded if an outbreak of similar events occurs. The firewall management system shall provide support for customizable attack or system alert event for monitoring or blocking.		
75	The firewall management system shall provide powerful reporting, including graphical representation of the end-to-end connections and packet capturing and troubleshooting capabilities.		
76	The firewall management system shall provide at least following Report Templates: System Report, Firewall Daily/Weekly Summary, Application Usage, Daily Threat Summary, Inspection Alert Daily Summary		
77	The firewall management system shall provide customizable reports to suit the specific needs of the environment.		
78	The firewall management system must be able to generate ad-hoc reports and also automate scheduled reports to be sent to administrators or managers on a daily, weekly or monthly basis. The firewall management system reporting shall allow administrator to customize their own report templates to display own company logo, style, etc.		

The Oriental Insurance Company Limited
Web Gateway

S.No	Features	Compliance (S/I/N)	Remarks
1	The solution should provide proxy, caching, on box malware inspection, content filtering, SSL inspection, protocol filtering and inline AV in block mode on the same Appliance.		
2	The Solution should be designed for user base in active-active mode managed through centralized management console on server platform.		
3	The Solution should provide HA and Load balancing functionality in Secure web gateway solution with or without any dependency on pac,external load-balancer or dns round-robin methods		
4	The solution should have complete license for Antivirus ,SSL, web security and content inspection and control should be built in solution for user base from the first day in same appliance. The Solution should intercepts user requests for web destinations (HTTP,HTTPs,and FTP) for web security and in-line AV scanning.		
5	The proposed solution should be able to inspect malicious information leaks even over SSL by decrypting SSL natively .The proposed SSL solution should be part of Gartner's Leaders/Challangers quadrant.		
6	The solution should be capable of dynamically blocking a legitimate website which has become infected and unblock the site in real time when the threat has been removed for below mentioned security categories and vulnerabilities.		
7	so Solution vendor should ensure to provide below mentioned security categories from day1 with automatic database updates for security categories- Advanced malware command and control, Advanced malware payloads, Bot networks, Compromised websites, key loggers, Phishing and other frauds, Spywares		
8	The solution should inspect the sensitive content through 1500 pre-defined templates, textual content inside image,commulative content control and inspection through web channel from day 1.		
9	The solution should have ability to protect the sentisitve data exfilatration based on geo-location.		
10	The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel.The solution should have ability to provide geo-location awareness for security incidents		
11	The solution should have at least 20+ million websites in its URL filtering database and' should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that 100 predefined categories & 100+ pre-defined protocols should be available on product from day-1. Also in-addition solution should have ability to configure custom categories for organization.		
12	The solution should have partnerships or third party inputs for web threat ratings from Virus total or Facebook		
13	The solution must detect and block outbound Botnet and Trojan malware communications. The solution must log and provide detailed information on the originating system sufficient to enable identification of infected units for mitigation		

14	The solution should support same policy enforcement in real time policy sync for users even when they access Internet outside the corporate network, this should be enforced through an agent deployment on roaming endpoints ((MAC/Windows) . And this solution should be on premises and not with the help of SAAS i.e. mobile user traffic should redirect to on-premise solution for policy checks. As per the security guidelines no SaaS or policy server public publishing should be allowed for the same.		
15	The agent on the roaming user machines should be tamperproof, for example, the agent cannot be uninstalled by the user even with admin rights to the system or the user cannot stop the services		
16	The solution should have ability to block anonymizer sites or proxy avoidance tools. Below mentioned tools should be blocked from first day and should be provided in default protocol database Ghostsurf, Google web accelerator, Hopster, Jap, Realtunnel, Socksonline, Tongtongtong, Toonel, Tor, Yourfreedom.		
17	Solution should provide separate Management server which can push policies for centralized management and reporting in case of multiple site solution deployment. Management console should provide automatic policy sync to all the remote boxes when the change is made to central console. Centralized management and centralized reporting console can be appliance based or software server hardware based but no VM should be used for the same.		
18	MAC OS X 10.10 and MS Windows 10 support for mobile laptop users web filtering client.		
19	The solution should have cloud application usage and associated risk visibility.		
20	The solution should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below RIGHT FROM FIRST DAY:1)Advanced Malware Command and Control category 2)Advanced Malware payload detection category 3)Malicious embedded links and iframe detection category 4)Mobile malware category 5)Key logger and Spyware category 6)P2P software database from day 1 to control/block the below P2P protocols		
21	The solution should filter out embedded objectionable or unproductive content, this includes examination of the source server, URL, page content, and active content. The solution should have functionality to control web 2.0 and real time content categorization.		
22	The solution should have granular control over popular social web applications like Facebook, Linkedln, Twitter, YouTube, and others. The solution should have social control Video UPLOADS to Facebook and YouTube applications.		

23	The solution must provide below mentioned categories or similar to functionally for Facebook control from day 1 Facebook Posting: Facebook function that enables a user to share a post, status or link, Facebook Commenting, Facebook Friends, Facebook Photo Upload, Facebook Mail, Facebook Events, Facebook Apps,Facebook Chat, Facebook Questions, Facebook Video Upload, Facebook Groups etc		
24	The solution should have built-in or custom policies for identifying and segregate You Tube traffic for Education only and Other irrelevant non-compliance video, It should simplify design and implementation of policy to ensure user compliance.		
25	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and uknown encryption files.		
26	The solution should be able to manage the complete solution through centralized management and reporting console which should be software or appliance based.		
27	The solution should support to have capability to differentiate between YouTube educational and entertainment videos through default categories and should have separate default categories for the same.		
28	The solution should have authentication options for administration, the specific permissions available depend on the type of administrator and Administrator activity is logged and available for auditing or troubleshooting.		
29	The solution should have authentication options for users/groups, It should supports authentication of users via Integrated Windows Authentication (Kerberos), NTLM (NTLM v1 and v2 in Session Security), and LDAP.		
30	The solution should have support of multiple domains, the administrators can specify the sequence (Domain controllers checked first, second, next, etc.) used to authenticate users who login from different locations.		
31	The solution should supports credential caching (for transparent and explicit proxy) to reduce load on domain controllers.		
32	The solution should have Multi-Domain authentication to allow the admin to create rules that authenticate against multiple domain controllers in a sequence		
33	The solution should have centralized management for multiple web egress points The solution should support for two factor Authentication for Management Server.		
34	The solution should support real time graphical and chart based dashboard for the summary of web filtering activities. The solution should pre-built report templates which the administrator can use for generating reports.		
35	The solution should have capabilities to automatically deliver reports based on schedule to selected recipients. The solution should support custom report creation in Excel and PDF.		
36	The solution should be able to consolidate reports from multiple boxes for centralized logging and reporting. The solution should provide detailed information on security incidents to comprehensively investigate individual threat events		

37	The solution should be integrated to third-party SIEM applications like syslog/CEF (ArcSight), syslog key-value pairs (Splunk and others), syslog LEEF (QRadar), and Custom.		
38	The solution should provide a Web UI to manage Internet usage policies, it should also support delegated administration and reporting capabilities so different roles can be created to manage policies and view reports.		
39	The solution should provide native system health monitoring, alerting and troubleshooting capabilities. The solution should provide reports based on hits, and bandwidth.		
40	The solution should support configuring scheduled automatic backup of system configuration. The solution should support automatic download of available patches or fixes		
41	The Solution should have inbuilt reporting feature like real time monitoring, reporting templates and investigation drill down report. The solution should have reporting on the user agent strings of applications to provide details on application usage and version details including browser version reports.		
42	The solution should be able to block back channel communication of sensitive data through default 1500 templates.		
43	The OEM Should in the Gartner leaders/challanger Quadrant for Secure web gateway solution. The OEM should have own T AC centre in India.		

The Oriental Insurance Company Limited
Antivirus

S.No	Features	Compliance (S/I/N)	Remarks
	Antivirus Protection and Other features		
1	Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.		
2	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.		
3	Must include capabilities for detecting and removing rootkits		
4	Must provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution		
5	Must have capabilities to restore spyware/grayware if the spyware/grayware is deemed safe		
6	Must have Assessment mode to allow first to evaluate whether spyware/grayware is legitimate and then take action based on the evaluation		
7	Must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process		
8	To address the threats and nuisances posed by Trojans, the solution should be able to do the following:		
	Terminating all known virus processes and threads in memory		
	Repairing the registry		
	Deleting any drop files created by viruses		
	Removing any Microsoft Windows services created by viruses		
	Restoring all files damaged by viruses		
	Includes Cleanup for Spyware, Adware etc		
9	Must be capable of cleaning viruses/malware even without the availability of virus cleanup components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether		
10	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients in case there is an outbreak		
	Behavior Monitoring		
11	Must have behavior monitoring to restrict system behavior, keeping security-related processes always up and running		
	enable Certified Safe Software Service to reduce the likelihood of false positive detections		
12	Must provide Real-time lock down of client configuration – allow or prevent users from changing settings or unloading/uninstalling the software		
13	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.		
14	CPU usage performance control during scanning		
	Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer		
	Adjusts the scanning speed if:		
	The CPU usage level is Medium or Low		
	Actual CPU consumption exceeds a certain threshold		

15	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually		
16	Should have Integrated spyware protection and cleanup		
17	Should have the capability to assgin a client the privilege to act as a update agent for rest of the agents in the network		
19	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)		
20	Safeguards endpoint mail boxes by scanning incoming POP3 email and Outlook folders for Threats		
21	shall be able to scan only those file types which are potential virus carriers (based on true file type)		
22	Should be able to detect files packed using real-time compression algorithims as executable files.		
24	Client machine acting as update agent which is delivering pattern updates to rest of the machines in the LAN, should have the capability to upgrade program upgrades also. No separate web server should be required		
25	Should have a provision for setting up a local reputation server so that for verifying reputation of any file, endpoints should not contact Internet always.		
26	shall be able to scan Object Linking and Embedding (OLE) File		
	Cloud computing		
27	Must Have in the cloud based protection and support for Online and Offline mode client protection		
	Must provide Web threat protection by the following ways:		
	Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings		
	Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location		
	Must have the capabilities to define Approved URLs to bypass Web Reputation policies		
	Must provide real-time protection by referencing online database with millions of rated Web domains		
	Configure Web reputation policies and assign them to individual, several, or all enduers machine.		
	Must provide File reputation service		
	Must be able to check the reputation of the files hosted in the internet		
	Must be able check the reputation of the files in webmail attachments		
	Must be able to check the reputaton of files residing in the computer		
28	Solution should work on the plugin architucture so that in future if we need to enhance the of our network we can do that without a major client level activity		
29	Must have smart feedback to enable feedback from the client agents to the threat research centers of the vendor.This will enable it to deliver automatic, real-time protection against the latest threats and provides "better together" security.		
30	Uses any alternate method other than the conventional pattern based scanning with the following features:		

31	Provides fast, real-time security status lookup capabilities in the cloud		
32	Reduces the overall time it takes to deliver protection against emerging threats		
33	Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud or some kind of repository and not to many endpoints		
34	Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.		
	Manageability and integration		
35	Must provide Comprehensive Support for Cisco Network Admission Control (CISCO NAC 1 & 2) with HCAP support		
36	Must provide seamless integration of the Cisco™ Trust Agent, enabling effective policy enforcement within a Cisco Self-Defending Network		
37	Must include a Policy Server for automated communication with Cisco Access Control Servers		
38	Should be able to deploy the Client software using the following mechanisms:		
	Client Packager (Executable & Microsoft Installer (MSI) Package Format)		
	Web install page		
	Login Script Setup		
	Remote installation		
	From a client disk image		
	Support MS Systems Management Server (SMS)		
39	Must provide a secure Web-based management console to give administrators transparent access to all clients and servers on the network		
40	The management server should be able to download updates from different source if required, which could be the vendor's update server, any other server or a UNC path		
41	If the update from the Management server fails, the security clients with the privilege should be able to get updated directly from the vendor's server		
42	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns		
43	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console		
44	Should have role based administration with active directory integration		
	To create custom role type		
	To add uses to a predifined role or to a custom role		
45	Shall support grouping of clients into domains for easier administration		
46	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)		
47	Shall offer centrally managed Client Firewall and IDS and also have virtual patching and it should be an automated process.		
48	Must be capable of unistalling and replacing existing client antivirus software (Provide the detailed list)		

49	Must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capabilities to clients and servers across the network		
50	All features (antivirus, anti-spyware, Enterprise Client Firewall and damage cleanup) are installed at the same time via client deployment methods and managed centrally via the web-based management console		
51	Security Compliance leverages Microsoft Active Directory services to determine the security status of the computers in the network		
	Platform Support		
52	Windows XP SP3 32-bit Edition		
53	Windows 2003 32-bit Edition		
54	Windows XP/2003 64-bit Edition		
55	Windows Vista (32-bit & 64-bit)		
56	Microsoft Windows Storage Server 2003		
57	Windows 7, 32-bit version & 64-bit version		
58	Microsoft Cluster Server 2003		
59	Windows Server 2008 and Windows Server 2008 R2, 64-bit version		
60	client installation on guest Windows 2000/2003/2008 operating systems hosted on the following virtualization applications:		
	VMware ESX/ESXi Server 3.5 or 4 (Server Edition)		
	* VMware Server 1.0.3 or later (Server Edition)		
	* VMware Workstation and Workstation ACE Edition 6.0		
61	Should support Intel x64 processor & AMD x64 processor		
62	Should support wireless devices such us Palm, Pocket PC, and EPOC at no extra cost		
63	Virtual Desktop Support : Solution should support Virtual Desktop for the following platforms:		
	· VMware vCenter™ 3.5 and 4 (VMware View™ 4)		
	· Citrix™ XenServer™5.5 and 5.6 (Citrix XenDesktop™ 4)		
	Notification, Reporting and logging		
64	Must be able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via E-mail, Pager, SNMP trap or Windows NT Event log		
65	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from personal firewall, and/or network virus logs exceed certain thresholds, signaling a possible attack.		
66	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack		
67	Solution Should have the capability to Protect sensitive data from unauthorized access and leakage from endpoint with the help of Antivirus Agent only by license upgrade. And also have focused on protecting the users from the external threat of data stealing malware. So that if required in future can use this feature with the need to any other resource		

The Oriental Insurance Company Limited
HIPS

S.No	Features	Compliance (S/I/N)	Remarks
1	Solution should support **Firewalling**		
2	Solution should support **Deep Packet Inspection (HIPS/HIDS)**		
3	Solution should support Anti Malware		
4	Solution should support Integrity monitoring		
5	Solution should support Log inspection		
6	Solution should also support Server-based licensingfor installation on physical/standalone servers.		
	Firewalling		
8	Firewall should have the capability to define different rules to different network interfaces.		
9	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, etc. and should detect reconnaissance activities such as port scans.		
10	Solution should provide policy inheritance exception capabilities.		
11	Solution should have the ability to lock down a computer (prevent all communication) except with management server.		
12	Firewall should integrate with Hypervisors like Vmware ESXi without the need to install agents on the guest VMs		
13	Solution should have Security Profiles allows Firewall rules to be configured for groups of systems, or individual systems. For example, all Windows 2003 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers.		
14	The solution should protect against Distributed DoS attacks		
	Deep Packet Inspection		
15	HIPS should integrate with Hypervisors like Vmware ESXi and NSX without the need to install agents on the guest VMs		
16	Host based IDS/IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window.		
17	Virtual Patching should be achieved by using a high-performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.		
18	Should provide automatic recommendations against existing vulnerabilities, Dynamically tuning IDS/IPS sensors (Eg. Selecting rules, configuring policies, updating policies, etc...) and provide automatic recommendation of removing assigned policies if a vulnerability no longer exists - For Example - If a patch is deployed		
19	Detailed events data to provide valuable information, including the source of the attack, the time, and what the potential intruder was attempting to exploit, should be logged		
20	Solution should be capable of blocking and detecting of IPv6 attacks.		
21	Solution should offer protection for virtual or physical, or a combination of both the environment		
22	The solution OEM should deliver virtual patching updates within 24hours of an application vendor announcing a vulnerability in their system		

23	The solution should have Application Control rules provide increased visibility into, or control over, the applications that are accessing the network. These rules will be used to identify malicious software accessing the network and provide insight into suspicious activities such as allowed protocols over unexpected ports (FTP traffic on a mail server, HTTP traffic on an unexpected server, or SSH traffic over SSL, etc.) which can be an indicator of malware or a compromise.		
24	Solution should provide policy inheritance exception capabilities.		
25	Product should support CVE cross referencing when applicable		
26	Solution should have Security Profiles allows rules to be configured for groups of systems, or individual systems. For example, all Windows 2003 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers		
	Anti-Malware		
27	Solution should support integration with Hypervisor components such as vshield endpointAPI (EPSEC) and provide Agentless AntiMalware protection for guest VMs		
28	Agentless Antivirus should support both Real Time and Schedule scan		
29	Solution should have flexibility to configure different real time and schedule scan times for diff guest VMs		
30	Agentless Antivirus Solution should have cloud-based threat intelligence combined with traditional endpoint security technologies		
31	Solution should also support restoration of quarantined files.		
32	Solution should support hypervisor level caching and de-duplication during Anti-Malware Scanning for improved performance		
	Integrity Monitoring		
33	Solution should support integration with Hypervisor components such as vshield endpointAPI (EPSEC) and provide Agentless AntiMalware protection for guest VMs		
34	Integrity Monitoring module should be capable of monitoring critical operating system and application elements (files, directories, and registry keys) to detect suspicious behavior, such as modifications, or changes in ownership or permissions.		
35	Solution should have extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc).		
36	Solution should be able to track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored.		
37	Solution should have Security Profiles allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Windows 2003 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers. However, each server has unique requirements which are addressed at the individual Host configuration level.		

38	Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.		
39	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, dns, etc..) and support custom rules as well		
Management and Other Features			
40	Management Server should support Active Passive high availability configuration for DC/DR setup		
41	The solution should be able to deliver all the above mentioned Firewall, Integrity Monitoring features through a single agent		
42	The solution should be able to automatically discover if any new agents are installed on any servers		
43	Solution should have single centralized web based management console.		
44	Solution should support application of policies during a scheduled day/time		
45	The solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the solution and who can do what within the application		
Log Inspection			
46	Solution should have a Log Inspection module which provides the ability to collect and analyze operating system, databases and applications logs for security events		
47	Solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow creation of custom log inspection rules as well.		
48	Solution should have Security Profiles allowing LogInspection rules to be configured for groups of systems, or individual systems. For example,all Windows2003 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers		
49	Product should be EAL4+ certified		

The Oriental Insurance Company Limited
Storage

Sr.No.	Make and model	Compliance (Yes/No)	Remarks
1	The offered storage should **have capability of** unified storage which supports Block and File data from a single management console. Also support the protocol like FC, iSCSI, NFS and CIFS.		
2	The Storage Systems should be Enterprise Class Storage System and supplied with minimum **8 TB** usable capacity.		
3	The proposed storage should also support 400GB SSD /Flash / FMD or Higher capacity or SAS disks: 600GB or higher capacity and NL-SAS disks : 6TB or higher Capacity		
4	The supported disks should be dual ported with minimum 6Gbps or higher full-duplex data transfer capability		
5	The Storage should be scalable to at least 100 disk drives under the single set of controller without replacing the controller.		
6	The offered storage should support for minimum **100000** IOPS with 80:20 Read/Write ratio from day one without Tiering, snapshot, cloning and replication overhead. OEM has to submit internal/External benchmark/tool report along with undertakiing on letter head.		
7	The Storage should support RAID 5, RAID 6, RAID10 etc.		
8	Storage System should have multiple Global Hot Spares.One Hot spare disk should be provided for every 30 Disk Drives		
9	Storage should support up to 8 x FC ports (16 gbps) for host connectivity		
10	Storage should have minimum **4x 12Gbps** SAS Links for Disk connectivity		
11	The storage system should have minimum **16 GB** per controller global cache total 64GB withing same set of controllers. Only write cache must be mirrored. .		
12	The storage should be with No Single Point of Failure (SPOF). All the components should be redundant and hot swappable including power supply, fans, batteries etc. The proposed storage must support non-disruptive replacement of hardware component		
13	The storage must provide non-disruptive firmware/micro code upgrade, device reallocation and configuration changes.		
14	The storage system should have support for multi-path configuration for redundant path to connected hosts. Any Licenses (unlimited/frame based) required for this should be provided with Storage.		
15	The storage should have protection of cache data during a power down by destaging the data in cache to non-volatile Disk.		
16	The storage should have Virtual/Thin provisioning and traditional raid group provisioning for Storage allocation to hosts.		
17	The storage should support dynamic LUN expansion/concatenation while LUN is mounted on the host		
18	The storage should support data tiering between different storage tiers namely SSD, SAS, and NL-SAS within the same storage array. Tiering license for **10TB** should be included in the proposal.		
19	The storage should be able to generate audit logs to record activities including host-initiated actions, physical component changes, attempts blocked by security control.		
20	The storage should have LUN masking or equivalent feature to prevent access of a LUN from unauthorized Hosts.		
21	The storage should support multiple operating systems such as Windows, Unix, Linux, Solaris etc. on a single port		
22	The storage should support clustering solutions such as Microsoft cluster, MS SQL cluster, SUN Solaris cluster, Linux cluster etc.		

23	The storage should have integration with major Database like Oracle, MS-SQL, My-SQL, DB2 etc to take application consistent copies when doing replication. Any Licenses for this support must be provided with System.		
24	Storage should support VMware vStorage API for Array Integration including but not limited to VAAI, VVOL, VASA etc. and ODX for Microsoft Hyper-V.		
25	The storage should be supplied with Storage management, virtual/thin provisioning, local copy (clone and snapshots both), Sub-Lun Data Tiering and other required software to meet the technical requirements. The storage should provide Sync and Asysnc replication Snapshot & clones license to be supplied for **10TB** of usable capacity.		
26	**Storage Management Features**		
a	Storage management software should be browser based/ web enabled accessible over IP		
b	Storage management s/w should have roles based access for user accounts to the storage system.		
c	Storage management software should provide interface/wizards to perform configuration operations like create LUNs present LUNs to host, set LUN attributes etc.		
e	Storage management software should be able to configure and manage tiering and auto-tiering		
f	Storage management software should be able to monitor alerts		
27	Snapshot and Cloning features		
a	The storage should support local copy of single source device to at least three or more target devices with background copy.		
b	The proposed storage should have point-in-time copy or snapshots		
28	The Proposed storage system must support partitioning of resource in logical and physical level that is covering Front end ports, Cache and logical volume		
29	Offered Storage array shall support heterogeneous storage virtualization (native/external) for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with **50TB**. In case of non-native/external component used, it should be supplied in redundant mode with no single point of failure.		
30	The offered storage vendor should be placed latest Gartner's Magic Quadrant Report report for Enterprise Class Storages.		

The Oriental Insurance Company Limited
SAN switch

Sr.No.	Make and model	Compliance (Yes/No)	Remarks
1	Minimum **16** Active ports should be available for DC and **16** Ports activated for DR. (each with minimum port speed **8** GbPS)		
2	Two nos. of Fibre channel switch should be provided in high availability mode.		
3	Minimum15 meter each and accessories for connecting Servers /Devices to SAN with optical mode 4 or higher standard cables.		
4	Should have capability of ISL trunking of minimum 8 ports.		
5	Switch should have FC ports for the SAN connectivity. Bidder can also propose the overall solution with the support of FCoE		
6	All the ports should operate at 8Gbps and auto-negotiate to 8Gbps/4Gbps FC speeds.		
7	Should have fans & fixed power supply		
8	All the components like, SFPs, and cards should be hot swappable field replaceable units allowing nondisruptive maintenance.		
9	Should have Management Tools for administration and configuration.		
10	Switch shall support in built diagnostics, power on self test, command level diagnostics, online and offline diagnostics.		
11	Should support Port security and Port Zoning.		
12	Should support Secure Shell (SSH) (SSL).		
13	Should support multilevel security on console access prevent unauthorized users from altering the switch configuration		
14	Should support Fibre Channel trace route and Fibre Channel Ping for ease of troubleshooting and fault isolation		
15	The switch should be rack mountable.		
16	Should support features such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments.		
17	Switch shall support diagnostics features such as port mirroring, Syslog, Online system health, Portlevel statistics etc.		
18	Any other specification		
19	The storage should be able to generate audit logs to record activities including host-initiated actions, physical component changes, attempts blocked by security control.		
20	The storage should have LUN masking or equivalent feature to prevent access of a LUN from unauthorized Hosts.		
21	The storage should support multiple operating systems such as Windows, Unix, Linux, Solaris etc. on a single port		
22	The storage should support clustering solutions such as Microsoft cluster, MS SQL cluster, SUN Solaris cluster, Linux cluster etc.		
23	The storage should have integration with major Database like Oracle, MS-SQL, My-SQL, DB2 etc to take application consistent copies when doing replication. Any Licenses for this support must be provided with System.		
24	Storage should support VMware vStorage API for Array Integration including but not limited to VAAI, VVOL, VASA etc. and ODX for Microsoft Hyper-V.		
25	The storage should be supplied with Storage management, virtual/thin provisioning, local copy (clone and snapshots both), Sub-Lun Data Tiering and other required software to meet the technical requirements. The storage should provide Sync and Asysnc replication Snapshot & clones license to be supplied for **10TB** of usable capacity.		
26	**Storage Management Features**		

a	Storage management software should be browser based/ web enabled accessible over IP		
b	Storage management s/w should have roles based access for user accounts to the storage system.		
c	Storage management software should provide interface/wizards to perform configuration operations like create LUNs present LUNs to host, set LUN attributes etc.		
e	Storage management software should be able to configure and manage tiering and auto-tiering		
f	Storage management software should be able to monitor alerts		
27	Snapshot and Cloning features		
a	The storage should support local copy of single source device to at least three or more target devices with background copy.		
b	The proposed storage should have point-in-time copy or snapshots		
28	The Proposed storage system must support partitioning of resource in logical and physical level that is covering Front end ports, Cache and logical volume		
29	The offered storage vendor should be placed in the leader's quadrant of the latest Gartner's report for Enterprise Class Storages.		

The Oriental Insurance Company Limited
Tape Library

Sr.No.	Make and model	Compliance (Yes/No)	Remarks
1	Tape autoloader must support 8 Active Tape Slots with LTO6 data cartridges.		
2	It should support 20 Tb Native capacity and 50 Tb compressed Max. capacity (LTO-6/LTO7) @ 2.5:1 compression		
3	Minimum have 1 No. of Drives		
4	Must have bar code reader		
5	Tape autoloader Shall support Linear tape Operation (LTO) 5, 6 drives, Barcode reader.		
6	It must have FC (8Gb with LTO-5, LTO-6) LC connector or SAS (6Gb with LTO-5, LTO-6) SFF-8088 connector interfaces		
7	It must Supports highest-level AES 256-Bit Encryption support either via LME OR AME GLOBAL STANDARDS.		
8	ATL must have broad compatibility with storage software and hardware components.		
9	ATL shall have remote monitoring capability.		
	Tape autoloader shall have remote management and reporting.		
10	Any other software required to manage the tape autoloader shall be included.		

S.No.	Requirement	Compliance (S/I/N)	Remarks
1	The proposed DC co-hosting infrastructure should be of Tier-III (or higher).		
2	The floor level of data center should be at least 6 ft. above the ground level		
3	A separate rack dedicated for the OICL within the server room / Hall area		
4	The data center should have a load bearing capacity of minimum 750Kg/Sq m.		
5	Freight Lift- The data center should have a high capacity freight lift for ease of movement of servers and high density H/W devices		
6	The design for cooling infrastructure at the data center should be in line with standard guidelines to support high density cooling needs		
7	Air Quality in data center site should be of severity level G1 (mild) as per ISA-71.04		
8	The bidder shall have one of the following valid certification as on bid submission date for the proposed facilities:		
8.1	BS7799 – 3		
8.2	ISO 27001		
9	The proposed DC area (viz. the server room, telecommunication room, staging room, IT equipment storage facility) should not have been flooded due to any reason in the past.		
	Server Room Area		
10	Layout of proposed space to be provided ,The server room area should have a raised floor height of 2ft.		
11	The server hall height from raised floor to false ceiling should be at least 8ft.		
12	DC Power (UPS output/BANK power input)		
12.a	Uptime- target 99.98%		
12.b	committed 99.9%		
12.c	Frequency - 50 Hz +/- 1Hz		
13	Dust level less than 5 micron		
14	Access card entry for the server hall area		
15	The temperature in the server room should be maintained at 20 +/- 2 degree C		
16	The humidity at the data center should be maintained at 50% +/- 5% RH.		
17	The server hall should have advanced fire detection & suppression systems through systems like VESDA & FM 200/FE 227 respectively		
18	99.98% uptime is required for the DC environmental infrastructure		
19	Gate passes to enter DC and DR premises for OICL representatives- free of any cost.		
20	Audit reports of people accessing the server room should be available to OICL. Bidder can keep the standard access logs for 90 days and should be made available to OICL based on OICL's request		
21	Availability of single phase & three phase power to support OICL equipment in the caged area.		
22	The bidder shall provide the electrical cabling of the racks to be hosted in the proposed rack space area.		
23	A power meter that can measure the exact power consumption by the OICL's equipment shall be setup.		
24	Power should be available from two different power sources (PDUs)		
25	Two separate power paths from the two separate UPS to be provided to the server/network communication room		
26	UPS should be configured in redundant mode		
27	Power sockets will be made available by Bidder and Availability of single and three phase, 4 wire power system.		

28	32 amps and 64 amps power sockets will be made available by Service provider		
29	The entire solution have power supply from the transformer as the primary source and automatic switchover to DG set as a secondary source		
30	Rack should be provided with atleast 6 KVA of power per rack		
31	The bidder should be have adequate power and cooling requirement factored to accommodate the scale of the requirement in full rack configuration utilization (Consideration for area of each rack unit is 35 Sq. Ft)		
32	The proposed server hall area should be well covered in fire detection and suppression system		
Building Management System			
35	Entry and exit should be restricted and monitored and should also be in CCTV surveillance coverage		
36	Security for the building should be available 24*7 at the entry and exit levels		
37	Biometric access to the common entry to the server room/hall area should be available		
38	The data center should have microprocessor based system to detect water leakage within a short period of time and fire alarm system		
39	There should be CCTV monitoring for surveillance of the Vijaya Bank racks in the server hall area.Activities should be recorded and the archival should be kept for at-least 30 days. Thereafter it should be provided to OICL on CD/ kept in storage devices on requiement basis.		
40	Smoke detection and fire suppression for the building to be available		
41	All the building management system (BMS) activities are to be controlled centrally in a room specifically to be used for BMS activities. The vendor should manage the BMS activities on a 24*7 basis		
42	The doors for the server room/hall area, communication room, and other critical areas should be fire rated		
43	The Server room/ Hall should have precision air conditioning with redundancy or the bidder can provide in-row cooling.		
44	Redundant CRAC units to facilitate high density cooling needs		
46	The data center should have electronic rodent repellent systems with operation ability on varied frequency range		
47	The bidder should share the video monitoring data in case required by OICL within a period of 3 days post official request raised by OICL at no additional cost		
48	Diesel tanks (for generators)-the Data Center should have high density diesel tanks for ensuring 24hr power backup with contracts for fuel supply on demand		
Communication Area			
49	Telecom junction box, multiplexers of various service providers to be available in and around the building		
50	The co-hosting facility service provider should extend the link terminated by the link service provider on the junction box till the server room where the OICL equipment will be located at no extra cost throughout the contract period.		
Seating Space			
51	Bidder should be capable of providing Seating space for 1 seats at each DC and DRS Site which could be scalable to 5 seats at site		
52	The seating area provided to the OICL shall have the network connection facility available between the seating area and the OICL server hall/server room		
53	The network link required between seating area and OICL racks shall be provided within 2 hours of such request from the OICL.		

54	Adequate locker facility should be provided in the seating area. The seating area furniture should be modular furniture with Keyboard tray for each table		
55	The UPS / generator backup power facility should be provided to the proposed seating area. SP shall provide UPS backed up 3 power points per seat.		
56	The seating area should be provided with Water and a vending machine with minimum amenities such as tea & coffee at no additional cost		
57	Bidder should provide a storage cabinet of approximate 6 ft. x 3 ft. with multiple shelves to keep documents.		
58	The SP shall provide a separate space to accommodate Bank's Fire vault cabinet (2.5' width x 2.5' length x Height- 3.5') in the seating area.		

ISO 27001 and other certificate should be valid as on date

S.No	Specifications	Compliance (S/I/N)	Remarks
1	The MPLS network should be capable of running Voice, Video and Data simultaneously		
2	The Service Provider should have capability to run IPV4 and IPV6 (dual stack) on MPLS links from day 1. Upgrade to IPV6 if required will have to be without any extra cost to OICL.		
3	The MPLS network provided by Service Provider should be fully isolated from Internet traffic even if running on the same core/backbone. It is desired that same PE Router does not run on both customer MPLS traffic and Internet traffic. The MPLS network offered to OICL should not carry any internet routes. Service provider has to provide network topology showing how internet is provided on MPLS cloud.		
5	Various MPLS configurations made for OICL VPN by the Service Provider should be shared with OICL. The service provider should also allow audit of the same by OICL's Auditors or through external independent auditors appointed by OICL. Any high and medium risk Vulnerabilities pointed out in Audit should be immediately rectified by the service provider. All other vulnerabilities shall be rectified in consultation with OICL. Scope of Audit limited to the scope of work of the Contract.		
6	The service provider should ensure that the all links are configured properly as per OICL's requirement in co-ordination with OICL/OICL appointed Vendor		
7	The Service Provider should provide protection against all kinds of malicious attacks including DOS attacks, SYN attacks, smurf attacks etc as well as provide protection against all kinds of spoofing like VPN spoofing/IP spoofing etc.		
8	The Service Provider should provide support to OICL or its Authorized vendor while implementing VPN variants like IPSEC VPN/GETVPN/ DMVPN /Tunel-less VPN/ any such technology		
9	The Service Provider should run industry standard QoS/CoS and Traffic Engineering services in the MPLS backbone and the service provider should configure Qos/CoS as per OICL's requirement in their network.		
10	Proper Change management procedure must be maintained for all the configuration changes done for/affecting OICL Links. The same should be made available to OICL immediately/ on demand. All configuration changes should be traceable. All such changes should be carried out with prior permission from OICL.		
11	The last mile at all OICL's locations, should have full redundancy through last mile connectivity from 2 different POPs of the service provider.		
12	There should not be any dependency on running open standard routing protocols like BGP, OSPF, Static Routes, etc. between OICL's locations and PE Routers of the Service provider.		

13	The Service Provider must provide the MPLS links to OICL that must be on any to any route topology i.e., All of OICL‟s locations should be reachable to each other through MPLS network of the service provider and without having to be touch OICL‟s Core at DC/DR Site.		
14	The MPLS Network should support multicast in variants like dense mode, sparse mode etc.		
15	If at some location Service Provider provides last mile through other Network service providers, the total responsibility of Liaisoning, commissioning, maintaining the link including all the commercials involved should be taken care by the Service Provider.		
16	If the last mile is on wireless, Service provider has to ensure that no other Radio equipment causes interference to Wireless signals used for OICL's connectivity and the Radio equipment should not be able to trap the signals used for OICL's network.		
17	OICL will not be responsible for installation of any telecommunication infrastructure equipment like RF Antenna, Mast, MUX, Modem etc. at the last mile and if required the same should be provided/installed by the Service Provider. Cost involved for the same should be borne by the Service Provider. OICL at the most will provide space and UPS power to Modems/equipment that may be required to implement the connectivity at the last mile		
18	Service Provider should provide various options of last mile like WIMAX/RF/ etc wherever fibre/copper is not feasible. VSAT as the last mile will not be accepted.		
19	Service Provider should provide connectivity with minimum number of "hop" for all links.		
20	The bandwidth should be upgradable on request from OICL on selective basis. Bandwidth charges for the same shall be payable as per cost provided in Additional Bandwidth cost section of Appendix 3- BOM.		
21	Service provider should upgrade the links with minor disruption, depending on OICL's Requirement		
22	All the POPs from where the MPLS bandwidth is provided to OICL should have redundancy of equipment, links, power, backhaul connectivity etc.		
23	The proposed bandwidth for OICL must be dedicated (1:1) and on dedicated ports.		
24	The MPLS links should be available in full duplex mode which must be demonstrated to OICL whenever OICL wants.		
25	The Service Provider should have independent Network Operation Centre with 24x7 support to take care of the complete network management requirements. The service provider should furnish details of Toll Free number		
26	Service Provider has to provide portal to OICL which can be used to monitor the SLA parameters and log the Trouble tickets through the same. OICL should also be able to obtain standard reports on the MPLS links like Bandwidth usage, availability of links etc. through the portal or through any network monitoring tool provided by Service Provider for all the links provided.		

27	The Core MPLS backbone of Service Provider covering at least all the metros in India should be fully meshed. In addition to the core, the other part of MPLS backbone of the service provider covering all their POPs mentioned as above should have minimum mesh for full redundancy.		
28	The service provider should support/provide inter-Autonomous System override feature in their network.		
29	The Service Provider is responsible for liaising with government agencies or other departments to provide any licenses, approvals etc. that may be required.		
30	OICL will consider the successful provision of the link subject to satisfactory Acceptance Test. The methodology for the test will be at the discretion of OICL. Following tests may be adopted (included but not limited to):		
	a. BER test as per best practice / ITU standards.		
	b. Normal PING test.		
31	Minimum latency to be maintained at all links is 100 ms.		

The Oriental Insurance Company Limited
Backup Software

S.No.	Make and model	Compliance (S/I/N)	Remarks
1	The proposed Backup Solution must support Backup Master Server, Media Servers and Clients on various OS platforms such as Windows, Linux and UNIX. Also be capable of supporting SAN based backup/restore from Various platforms.		
2	Backup Software should provide, an online backup for all the database and applications i.e. Oracle, Exchange, Active Directory, Sharepoint, SQL, DB2, Sybase, Informix etc		
3	Proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration. The proposed backup solution software has inbuilt Java Or Web based GUI for centralized management of backup domain.		
4	Backup Solution should have inbuilt capability of de-duplication everywhere i.e. at Source, media & target and should not have any special disk (SSD) or high-end large RAM requirement for Deduplication.		
5	The proposed Backup Solution supports the capability to write up to 32 data streams to a single tape device or multiple tape devices in parallel from multiple clients to leverage the throughput of the Drives using Multiplexing technology.		
6	Should support various level of backups including full, incremental, differential, synthetic and optimized synthetic backups		
7	Capability to configure retries for backups of a clients in case the clients is not available on the network due to reboot or network failures. Backup software should also provide checkpoint restart feature so that both backup and restore jobs start from the point where the job failed rather than restart the entire job.		
8	Proposed backup solution should be in Gartner leaders quadrant, should be in the leaders quadrant for last 10 years		
9	The proposed backup solution shall support industry leading cluster solution such as MSCS, Service Guard, Veritas Cluster.		
10	Proposed Backup solution should support instant recovery (directly through backed up images) of virtual machines.		
11	The backup solution must provide file backup, Bare Metal restore, deduplication, encryption, database online backup, dedupe data replication etc with single agent. Multiple agents/clients should not be installed in server to achieve above features.		
12	The backup software must support TAR format for writing backup data to tapes.		
13	The proposed backup solution should support tape mirroring of the same job running concurrently with primary backup.		
14	The proposed backup solution must support at least AES 256-bit encryption capabilities.		
15	Should be able to backup open files on Windows and non-Windows Environment, and backup of other OS platforms like RHEL, SUSE Linux, AIX, Solaris & HP-UX		

The Oriental Insurance Company Limited
Core Router

Sr. No.	Item	Specification	Compliance (S/I/N)	Remarks
1	General Requirements	The router should support security, voice, IP routing, IP multicast, QoS, IP mobility, multiprotocol label switching (MPLS), VPNs, and redundant power supply.		
2	Hardware and Interface Requirements	Routers should have at least 1 open slots for LAN or WAN modules		
		Router should have minimum 2x 10/100/1000 GE ports to be configured. All onboard GE ports should also support SFP based ports to allow ISP to provide fiber based last mile if feasible.		
3	Performance Requirements	The router should have a minimum performance of upto 1 Gbps		
		Should support other IP Services like GRE tunneling, ACLs, NAT services		
4	Quality of Service (QoS)	Routers should support marking, policing and shaping		
		Routers should support Voice traffic optimization with features like WRED, QoS, & RSVP		
5	Routing Protocol	IPv4 and IPv6 tunneling enabled from day one		
		HSRP/VRRP, Static Routes, RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing enabled from day one.		
6	IPv4 Multicast features	Router should support IGMP v1/v2/v3, PIM-DM, PIM-SM, Source Specific Multicast (SSM) from day one		
7	System Management and Administration	Support for accounting of traffic flows for Network planning and Security purposes		
		Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP		
		Routers should support Software upgrades		
		Routers should support SNMPv2 and SNMPv3		
8	Security features	Routers should support AAA using RADIUS or TACACS+		
		Routers should support Packet Filters like: Standard ACL		
		Routers should support Tunnels (GRE, IPSec)		
9	Built-in troubleshooting	Extensive debugs on all protocols		
		Shall support Secure Shell for secure connectivity		
		Should have to support Out of band management through Console /an external modem for remote management/ USB port.		
		Pre-planned scheduled Reboot Facility		
		Real Time Performance Monitor – service-level agreement verification probes/alerts		
10	Certification	Should be UL/CE/IEC & EAL2/NDPP Certified		

The Oriental Insurance Company Limited
Core Switch

Sr. No.	Item	Specification	Compliance (S/I/N)	Remarks
1	General Requirement	Must have 24 Ethernet copper ports of 10/100/1000 Line Rate for 64 byte Packets with 2 NOs of SFP+ Modules of 10G ports(all ports are Unshared and fully populated)		
		RoHS compliant		
		CPU with clock speed of 600 MHz or more		
		1 GB Flash memory		
		512 MB RAM		
		At least 1 out-of-band management console over Ethernet RJ45		
		Redundant Power supply (fully populated)		
		1 U/2U Rack mountable		
		tack Support with stacking done over dedicated port.		
2	Performance	At least 88 G non-blocking switching bandwidth		
		At least 65 Mpps of forwarding rate for 64 bytes of packet		
		MAC address table supporting at least 16000 MAC Addresses		
		Routing table supporting at least 10000 IPv4 unicast routes		
		Support for at least 2048 configurable VLAN ID's with Switched Virtual Interfaces		
		Support for Jumbo Frames		
3	Layer 3 Features	Static and Dynamic routing protocols such as RI Pv2, OSPF, BGPv4 etc.		
		IGMPv2 and IGMPv3		
		IPv6 Routing protocols such as Static v6 and OSPFv3.		
		MLDv1 and MLDv2		
		Support for Dual stack and 6in4 tunnelling methods for IPv6 transition		
		IP Multicast and PIM, PIM Sparse Mode and preferably PIM dense Mode & Source-Specific Multicast for Clients		
		IPv6 & IPv4 Policy Based Routing (PBR)		
		Able to discover (on both IP v4 & IP v6 Network) the neighbouring routing device giving the details about the platform, IP Address, Link connected through etc.		
4	Layer 2 Features	Link Layer Discovery Protocol (LLDP)		
		Link Aggregation Control Protocol (LACP) or equivalent that allows the creation of Ethernet channelling(channel bonding) with devices that conform to IEEE 802.3ad		
		Voice VLAN		
		Traffic Mirroring based on PORT/VLAN to a local or Remote Switch		
		Dynamic VLAN Assignment		
		Private VLAN		
		Layer 2 redundancy and load balancing		
		IEEE 802.1sfw Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP)		
		832 q VLAN encapsulation		
		Auto-MDIx		
		Auto-negotiating on all ports to automatically select half or full-duplex transmission mode to optimize bandwidth		
5	Security Features	Port security to secure the access to an access or trunk port based on MAC address and to limit the number of learned MAC addresses to deny MAC address flooding		
		DHCP snooping		
		Flexible & multiple authentication mechanism e.g. 802 1X, MAC Authentication bypass.		
		VLAN ACLs on all VLANs to prevent unauthorized data flows from being bridged within VLANs		
		IPv6 ACLs to filter IPv6 traffic		
		Port-based ACLs for Layer 2 interfaces to allow security policies to be applied on individual switch ports		
		Switch should securely encrypt all access methods (CLI, GUI or MIB) through SSHv2/SSL, SNMPv3.		
		Bridge protocol data unit (BPDU) Guard or equivalent to shut down Spanning Tree Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops		
		Spanning Tree Root Guard (STRG) or equivalent to prevent edge devices not in the network administrator’s control from becoming Spanning Tree Protocol root nodes		
		Dynamic VLAN & MAC Based Filtering		
		DOS protection of Switch's Control Plane using rate limiting and ACLs.		
6	Quality of Service	802 p CoS and DSCP Field classification using marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 Transmission Control Protocol/User Datagram Protocol (TOP / UDP) port number and TOS		
		Rate limiting based on source and destination IP address, source and destination MAC address, Layer 4 TCP/UDP information or any combination of these fields		
7	Manageability	TACACS and RADIUS authentication to facilitate centralized control of the switch and restricts unauthorized users from altering the configuration		
		Multi level security on console access to prevent authorized users from altering the switch configuration		

		Embedded Remote Monitoring (RMON) software agent supporting four RMON groups (History, Statistics, Alarms and Events) for enhanced traffic management and monitoring		
		TFTP (Trivial File transfer protocol) or any equivalent method for easy firmware upgrades and backup on the network		
		Should be able to manage and monitor all Switches through a single management console.		
		Should support HTTP/Telnet/SSH for switch management		
		SNMPv1, v2c, and v3		
		NIP client (SNTP v4),DNS client, DHCP client and DHCP relay agent		
		Rollback option to rollback to previous saved configuration		
8	Application Visibility	Sflow ready		
		Capable of enabling Sflow on all ports of the switch for Ingress and Egress Traffic		
9	Standards and Compliance	IEEE 802.1 s		
		IEEE 802.1 w		
		IEEE 802.1 x		
		IEEE 802.1 ab		
		IEEE 802.3 ad		
		IEEE 802.1 D Spanning Tree Protocol		
		IEEE 802,1 P CoS Prioritization		
		IEEE 802.1 Q VLAN		
		IEEE 802.3 10 EASE-T specification		
		IEEE 802.3 u 100 BASE-TX specification		
		IEEE 802.3 ab 1000 BASE-T specification		
		IEEE 802.3 z 1000 BASE-X specification		
		RFC 2925		
		RFC 2131		
		RFC 3046		

The Oriental Insurance Company Limited
Internet Router

Sr. No.	Item	Specification	Compliance (S/I/N)	Remarks
1	General Requirements	The router should support security, voice, IP routing, IP multicast, QoS, IP mobility, multiprotocol label switching (MPLS), VPNs, and redundant power supply.		
2	Hardware and Interface Requirements	Routers should have at least 1 open slots for LAN or WAN modules		
		Router should have minimum 2x 10/100/1000 GE ports to be configured. All onboard GE ports should also support SFP based ports to allow ISP to provide fiber based last mile if feasible.		
3	Performance Requirements	The router should have a minimum performance of 400 Mbps		
		Should support other IP Services like GRE tunneling, ACLs, NAT services		
4	Quality of Service (QoS)	Routers should support marking, policing and shaping		
		Routers should support Voice traffic optimization with features like WRED, QoS, & RSVP		
5	Routing Protocol	IPv4 and IPv6 tunneling enabled from day one		
		HSRP/VRRP, Static Routes, RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing enabled from day one.		
6	IPv4 Multicast features	Router should support IGMP v1/v2/v3, PIM-DM, PIM-SM, Source Specific Multicast (SSM) from day one		
7	System Management and Administration	Support for accounting of traffic flows for Network planning and Security purposes		
		Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP		
		Routers should support Software upgrades		
		Routers should support SNMPv2 and SNMPv3		
8	Security features	Routers should support AAA using RADIUS or TACACS+		
		Routers should support Packet Filters like: Standard ACL		
		Routers should support Tunnels (GRE, IPSec)		
9	Built-in troubleshooting	Extensive debugs on all protocols		
		Shall support Secure Shell for secure connectivity		
		Should have to support Out of band management through Console /an external modem for remote management/ USB port.		
		Pre-planned scheduled Reboot Facility		
		Real Time Performance Monitor – service-level agreement verification probes/alerts		
10	Certification	Should be UL/CE/IEC & EAL2/NDPP Certified		

The Oriental Insurance Company Limited
Internet Switch

Sr.No.	Specifications	Compliance (S/I/N)	Remarks
1	19" Rack Mountable stackable switch with min 24 Nos. 10/100/1000BaseT with Min. 2Nos. free SFP/GBIC slot to accommodate 1000Base-Sx/ 1000Base-Lx Ports		
2	It should support all L2 functionalities along with SNMP & port level security. Should be IPV6 ready.		
3	Switch should support for minimum 48 Gbps of throughout & minimum 35 mpps forwarding rate		
4	The switch should have dedicated stacking port /module for stacking		
5	The switch should have IPV4 & IPv6 support & configured for the same		
6	Switch shall support IEEE 802.3ad Link Aggregation Control Protocol (LACP)		
7	It shall support IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP or equivalent technology and static routes.		
8	Switch should support IGMP v1/v2/v3 as well as IGMP snooping & SNMP v1,v2 and v3		
9	Switch should have feature to protect access ports using port security, TACACS+/Radius, storm control, Access Control List.		
10	Switch should support queuing as per IEEE 802.1P standard on all ports with mechanism for traffic shaping and rate limiting features for specified Host, network, etc.		
11	The switch should suppoort basic routing static, RIP, Inter-Vlan Routing , IGMP Snooping, from day one . The swicth should be capable of supporting advance Routing sush as OSPF and PIM in future based on the requirement.		
12	Should be UL/CE/IEC & EAL2/NDPP Certified		

The Oriental Insurance Company Limited
Desktop

Sr.	Specification		Compliance (S/I/N)	Remarks
	Intel Core i5 processor based PC with TFT			
1	CPU	Intel® Core™ i5-6500 Processor (3.2 GHz, 6M Cache)or higher		
2	Mother Board	Intel Chipset with Intel/OEM Motherboard		
3	Memory	4 GB DDR4 RAM expandable to 16 GB or higher		
4	BIOS	Flash BIOS		
5	Ports	2 external USB 3.0 ports, 4 external USB 2.0 ports, 3 PCI / PCI Express with at least 1 PCI Express x16 slot , 1 RJ-45, 1 VGA, 1 HDMI/DVI/Display Port, 1 serial port and 1 parallel on-board or through convertor		
6	Networking Feature	Integrated LAN –10/100/BaseTx Mbps speed		
7	HDD	Serial ATA 6.0 Gb/s 500 GB HDD (7200 rpm) or higher.		
		Support for future expandability 1 TB HDD in future.		
8	Graphics	Integrated Intel Graphics or higher		
9	Audio	Integrated High Definition Audio		
10	Monitor	18.5" LED Blacklit Color Monitor TFT (Same make as PC) (Energy star/TCO 06 compliant)		
11	Keyboard/ Mouse	USB Keyboard (Same Make as PC) and Optical USB Mouse (Same make as PC)with Mouse PAD		
12	Operating System Support	Microsoft Windows 10 professional - 64 bit down gradable to Windows 8.1/7 Professional 32/64 bit with CD Media (capable of reloading OS with all drivers' software even in case of Hard disk failure)		
13	Security	Security lock on chassis for physically securing the chassis. Power -On Password, Setup Password, Memory Change Alert functionality with Pad lock.		
14	Features	Manageability features like Serial No, Make, Model details of (BIOS, HDD, Memory, O/S Information), Pre-failure HDD Alert etc.		
15	Certificate	ISO 9001:2008 or higher Certified		
16	Certificate of Authenticity	Serial Numbers of the machines along with DPK should be supplied to the Bank for Windows 8/Certificate of Authenticity of Microsoft Windows mentioning OEM name should be supplied for Windows7		
17	System Protection	System Protection tool to significantly increase the uptime in most of the situations mentioned As under-		
		· Accidental file deletion		
		· Format of any partition of HDD		
		· Corruption of registry files/link files		
		· Uninstall of software & applications		
18	Regulatory Standards	FCC/UL Equivalent, ROHS , Energy Star 6 compliant or equivalent		

The Oriental Insurance Company Limited
Printer-BW

Sr.	Specification		Compliance (S/I/N)	Remarks
1	Make and model must be specified			
2	Print speed(Black Normal A4)	25 to 30 PPM		
3	Resolution	Minimum 600X600 dpi		
4	RAM	Min 128 MB		
5	First page out	Less than 10 second		
6	Paper Tray	150 sheets or above input tray 100 sheets or above output tray		
7	Media size	A4, Letter, Legal		
8	Interface	USB 2.0 or higher with cable		
9	Operating System compatibility	Windows, Linux, OCR software, Searchable PDF		
10	Monthly Duty Cycle	10000 pages or above		

simplex with Network

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above Laser Printer A4 25-30 ppm black with Network (10/100/BaseTx Fast Ethernet)		

simplex with Wifi

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above Laser Printer A4 25-30 ppm black with wifi		

Automatic Duplex

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above Laser Printer A4 25-30 ppm black duplex		

Automatic Duplex with network

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above Laser Printer A4 25-30 ppm black duplex with network		

Automatic Duplex with Wifi

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above Laser Printer A4 25-30 ppm black duplex with wifi		

The Oriental Insurance Company Limited
Printer -Color

Sr.	Specification		Compliance (S/I/N)	Remarks
1	Make and model must be specified			
2	Print speed	30-35 PPM Colour & Black		
3	Resolution	Min 1200X1200 dpi		
4	RAM	Min 512MB		
5	First page out	Less than 11 second		
6	Paper Tray	500 sheets on standard input tray, 100 sheets on multipurpose tray		
7	Media size	A4, Letter, Legal		
8	Interface	High Speed USB 2.0 with cable		
9	Operating System compatibility	Windows, Linux and Mac		
10	Monthly Duty Cycle	75,000 pages or above		
11	Duplex	Automatic Duplex capability		
12	Network Interface	10/100/BaseTx Mbps fast Ethernet interface		

The Oriental Insurance Company Limited
MFP

Sr.	Specification		Compliance (S/I/N)	Remarks
1	Make and model must be specified			
2	Function	Print, copy, scan		
3	Memory	Minimum 256MB		
4	Duplex	Manual		
5	ADF	Built in automatic minimum 30 sheets or above		
6	Print speed	A4- Minimum 25 – 30 PPM		
		A3 - 20-25 PPM		
7	Resolution	Min 600x600 dpi		
8	Paper tray	Minimum 250 sheets input tray Minimum 100 sheet output tray		
9	Monthly Duty	**30**000 pages or above		
	Cycle- A4			
10	Media size	A4, letter, legal		
11	Scan	Flatbed ADF – Dual side scanning		
12	Scan resolution	Min. 600x600dpi		
13	Scan file format	JPEG, PNG, PDF		
14	Scan speed normal	20 ppm or above		
15	Copier speed	15 ppm or above		
16	Copier resolution	600x600dpi		
17	Reduce or enlarge	Min 25% to 400% or above		
18	Interface	USB		
19	Operating system compatibility	Windows, Linux and Mac, OCR software, searchable PDF		

simplex with Network

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above MFP Laser Printer A4- 25-30 ppm color with Network (10/100/BaseTx		

simplex with Wifi

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above MFP Laser Printer A4- 25-30 ppm color with wifi		

Automatic Duplex

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above MFP Laser Printer A4 25-30 ppm black duplex		

Automatic Duplex with network

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above MFP Laser Printer A4 25-30 ppm color duplex with network		

Automatic Duplex with Wifi

S.no	Parameter	Compliance (S/I/N)	Remarks
1	Above MFP Laser Printer A4 25-30 ppm color duplex with wifi		

The Oriental Insurance Company Limited
Scanner

Sr.	Specification		Compliance (S/I/N)	Remarks
1	Make and model must be specified			
2	Scanner Type	ADF		
3	Scanning Speed	25-30 ppm / 50-60 ipm – A4		
4	Scan Type	Color & B/W –ADF		
5	Duplexing Scanning	Auto Duplex Scanning		
6	Scan Resolution	600x600 dpi (optical) or higher		
7	ADF Capacity	Minimum 50 Pages or above		
8	Interface	USB 2.0 or higher with cable		
9	Software	Suitable software for Image and Document scanning, editing and should be able to save in standard formats e.g. BMP, TIF, JPG, PDF, RTF. Software to be compatible with Windows 7, 8.1, 10, RHEL (optional) and required drivers. OCR software, searchable PDF.		
10	Duty Cycle	Min 3000 pages per day		

The Oriental Insurance Company Limited
Projector

#	Specification	Compliance (S/I/N)	Remarks
1	Power Supply: 220 to 240 V AC, 50/60 Hz		
2	Resolution: Min 1024 x 768		
3	Computer Compatibility: VGA (640 x 480) to WUXGA (1920 x 1200)		
4	Projection Size: Min. range 30” to 300”		
5	Compatibility with Computer OS: Win 7 onwards, Linux, Apple Mac		
6	Lamp Life: Min. 2000 Hrs.		
7	Brightness: Min. 3500 lumens		
8	On Screen Menu: English		
9	Contrast Ratio: Min. 500:1		
10	Aspect Ratio: Min. 4:3		
11	Accessories: Power cord, VGA cable, wireless remote control, Remote Batteries, Carry Bag, HDMI Cable, Lens Cover etc.		
12	Screen/Wall Mounted: Yes		

The Oriental Insurance Company Limited
UPS

S.No	Item	Specification	Compliance (S/I/N)	Remarks
1	**Input Source**	Mains/ Local make DG set		
2	**Rating**	Input rating VA: Not less than 0.90 at full load with P.F. Correction		
3	**Input Voltage**	160 V to 270 V for Single Phase and 345V to 465V for phase to phase		
4	**Input frequency**	47 - 53 Hz		
5	**Input Phase**	10 KVA (Single Phase)		
6	**Output Voltage**	230V +/- 2% (both for load and supply variations) (Base Voltage adjustable)		
7	**Frequency**	50 Hz +/- 0.5% (Constant frequency Output)		
8	**Waveform (Output)**	Sine Wave from with THD less than 3%		
9	**Isolation**	UPS input should have true Galvanic isolation through transformer only		
10	**Transient Response**	Less than 40 milliseconds for 0 to 100% step load change		
11	**Minimum metering**	1. Battery Voltage		
		2. Battery Low Audio Alarm		
		3. Output OK indicator		
		4. Input / Output voltage meters; Input/ Output Frequency		
		5. Load Utilization Indicator		
12	**LED Indicators**	UPS on Mains/ Battery - Mains On, Inverter ON, Battery On charge, Low battery Eminent, DC Over/under		
13	**Inverter efficiency**	Greater than 90%		
14	**Overall efficiency**	Greater than or equal to 80%		
15	**UPS type**	Online (to act as Power conditioner as well as Backup)		
16	**Inverter Technology**	Switch mode (PWM with IGBT Switches)		
17	**Battery Charger**	Current emitted maximum voltage equal to 2.33 V per cell		
18	**Over Load Capacity**	110% for 60 min		
		125% for 1 min		
		150% for 1 sec		
19	**Maximum Charging Current**	Not to exceed 10% of Battery Capacity		
20	**Battery Type**	SMF (VRLA Type)* Non Calcium Type		
21	**Nominal Voltage**	At least 180V DC for Single phase and At Least 240 V DC for three phase		
22	**Battery make**	The battery OEM should be a reputed company having brand name in the market with ISO mark i.e. ISO 9000		
23	**Recharge Time**	< 10 hours from fully discharged to 100% charged condition		
24	**Battery Life**	Min 3-5 Years; Warranty 36 months		
25	**Backup Time**	30 Min.		
26	**General Protection**	Input Over/under Voltage, DC Over/Under Voltage. Inverter Over/Under Voltage, Inverter Overload, Overheat,		
27	**PC interface (Optional)**	USB / RS 232 with SNMP card Compatibility. UPS system should have the provision for integrating the features /		
28	**Protection class**	IP-21		
29	**Temperature**	0o C – 45o C		
30	**Humidity**	0-60% (Non-Condensing)		
31	**Dimensions**	To be specified by the vendor		