Server:	DL360 Gen10	
Item	**Description of Requirement**	**Compliance**
Chassis	1U Rack Mountable	
CPU	(2.4GHz/10-core) processors	
CPU L3 CACHE Memory	8.25 MB L3 cache to 38.5 MB L3 cache depending upon processor model chosen	
Motherboard	Intel® C621 Series Chipset	
Memory	128 GB DIMMS scalable upto 1.5 TB using DDR4 Load Reduced DIMM (LRDIMM) operating at 2600 MHz .	
Memory Protection	memory and fast fault tolerance	
HDD Bays	or 10 NVMe PCIe SSD The drive carrier should have intutive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to aviod dataloss/downtime due to wrong drive	
Hard disk drive	2 Nos 3TB and above Hot Plug SFF drives	
Controller	supporting SSD/HDD and at least two M.2 drives In addition, server should support one of the below controllers supporting Mixed Mode which combines RAID and HBA mode, PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0/1/1+0/5/50/6/60/1 Advanced Data Mirroring/10 Advanced Data Mirroring (onboard or on a PCI Express slot) or PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID	
Networking features	Server should support below networking cards: 1. 1Gb 4-port network adaptors 2. 10Gb 2-port Ethernet adaptor 3. 10GBaseT 4-port Ethernet adaptor 4. 4x25Gb Ethernet adaptor 5. 10/25Gb 2-port Ethernt adaptor Infiniband Options: 40Gb dual port or 100Gb Single or Dual port Adapter 100Gb Single port Omni path adaptor	
Interfaces	Micro SD slot - 1 USB 3.0 support With Up to 5 total: 1 front, 2 internal, 2 rear, 2 internal (secure)	
Bus Slots	Three PCI-Express 3.0 slots, atleast two x16 PCIe slots	
Power Supply	minimum 94% efficiency	
Fans	Redundant hot-plug system fans	
Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support USB 2.0 Support Energy Star ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum) SMBIOS Redfish API IPMI 2.0 SNMP v3 TLS 1.2 DMTF Systems Management Architecture Active Directory v1.0	

System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 TPM (Trusted Platform Module) 2.0 Bezel Locking Kit option	
Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ClearOS	
GPU support	and graphics accelerators	
System tuning for performance	for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode 2. System should support workload Profiles for simple performance	
Secure encryption	the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for	
Warranty	support with next business day response.	
Provisioning	discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting	
Firmware security	management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid	
Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 3. Server should support agentless management using the out-of-band remote management port 4. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 5. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be availabile 6. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay	
	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.	
	following: • Server Profiles • Server Hardware • Appliance alerts	
	access control	

Server Management	virtualization platform management software like vCenter, and SCVMM	
	component failure alerts on critical components like CPU, Memory and HDD.	
	The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contrats and status. The Portal should also provide a Personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of	
	Server Management agents and enable the remote update of system software/firmware components.	
	of the server supplier.	