بسم الله الرحمن الرحيم

ނޭޝަނަލް ސެންޓަރ ފޯރ އިންފޮރމޭޝަން ޓެކްނޮލޮޖީ

ބީލަން ފޯމް

ޕްރޮކިއުމަންޓް ނަން	އެސްޑީ ވޭން (SD-WAN) ގަތުމަށް
ޕްރޮކިއުމަންޓް ނަންބަރު	PROC-2023-01
އިޢުލާން ނަންބަރު	(IUL) 164-PRO/1/2023/8
ތާރީޚް	*30 ޖެނުއަރީ 2023*

1. ތަފާސް ދިނުމުގެ ގޮތް		
1.1. ތަފާސް		ހިންގާ ފަރާތުން ކަންކަން ބަލަހައްޓަންވީ/ ދިރާސާ ކުރަންވީ ގޮތް
1.2. ތަފާސް	ނަންބަރު	(IUL) 164-PRO/1/2023/8
	ތަފާސް ފެށޭ	30 ސެޕްޓެމްބަރ 2023
	ތަފާސް ކުރާ ގޮތް	ކުރިއަރުވާ ތަފާސް ގެ ދަށުން ކުރެވޭ ތަފާސް ކަމުގައި
1.3. ތަފާސް ކުރާނެ ގޮތް	ގޮތް	ކުރިއަރުވާ ތަފާސް ގެ ދަށުން ކުރެވޭ
	ތަފާސް ކުރާ	NCIT ތަފާސް ކުރާ، 64 ބަސް ބޭނުން، ކަނޑައެޅިފައި ހުންނަ
	ފުރިހަމަ ކުރަން ޖެހޭ	2023 ފެब്രുവരി 19 ވ ފުރިހަމަ ވަގުތު 10:00 ގެ ކުރިން NCIT ގެ ބިލްޝޯދަށް ދަތުރުކުރާ ފަރާތްތަކުގެ ފާސްކޮށް ހުންނަންވާ ތަފާސް ކުރާ ގޮތް ތަކެއް ހުންނަންވާނެ. ތަފާސް ފެށުމުގެ (2023 ފެब്രുവരി 19 ވ ފުރިހަމަ) ހަމަވާ ގަޑި، ގިނަ ގޮތެއް ނަމަ 10:00 ގެ ކުރިން NCIT ގެ ބިލްޝޯދަށް ދަތުރުކުރާ ފަރާތްތަކުގެ ފާސްކޮށް ހުންނަންވާ ތަފާސް ކުރާ ގޮތް ތަކެއް ހުންނަންވާނެ.
1.4. ތަފާސް ކުރާ ގޮތް	ގޮތް	ކުރިއަރުވާ ތަފާސް ގެ ދަށުން ކުރެވޭ
	ތަފާސް ކުރާ	NCIT ތަފާސް ކުރާ، 64 ބަސް ބޭނުން، ކަނޑައެޅިފައި ހުންނަ
	ފުރިހަމަ ކުރަން ޖެހޭ	2023 ފެब്രുവരി 19 ވ ފުރިހަމަ ވަގުތު 10:10 ގައި، ދިރާސާ ތަފާސް ކުރާ ފަރާތުން ތަފާސް ކުރާ ގޮތުގެ ކުރިން ދައްކަންވާ ފައިސާ ދައްކާ ގޮތުގެ ލިޔުން ހުށަހަޅާ ފާސްކޮށް ދައްކާ ގޮތުގެ ލިޔުން ހުށަހަޅާ ފަރާތްތަކުގެ ލިސްޓު ތަފާސް ކުރާ ގޮތުގެ ކުރިން ދައްކަންވާ ފައިސާ ދައްކާ ގޮތުގެ ލިޔުން ހުށަހަޅާ ފަރާތްތަކުގެ ލިސްޓު ތަފާސް ކުރާ ގޮތުގެ ކުރިން ދައްކަންވާ ފައިސާ ދައްކާ ގޮތުގެ ލިޔުން ހުށަހަޅާ ފަރާތްތަކުގެ ލިސްޓު (2023 ފެब്രുവരി 19 ވ ފުރިހަމަ) ހަމަވާ ގަޑި، ގިނަ ގޮތެއް ނަމަ 10:10 ގައި، ދިރާސާ ތަފާސް ކުރާ ފަރާތުން ތަފާސް ކުރާ ގޮތުގެ ކުރިން ދައްކަންވާ ފައިސާ ދައްކާ ގޮތުގެ ލިޔުން ހުށަހަޅާ ފަރާތްތަކުގެ ލިސްޓު ތަފާސް ކުރާ ގޮތުގެ ކުރިން ދައްކަންވާ ފައިސާ ދައްކާ ގޮތުގެ ލިޔުން ހުށަހަޅާ ފަރާތްތަކުގެ ލިސްޓު

2. ފާސްކުރުމުގެ ގޮތުގައި ބޭނުންކުރާ ތަފާސް ކުރާ ގޮތާ ބެހޭ ތަފާސް	
2.1.	ދިރާސާ ތަފާސް ކުރާ ފަރާތުގެ ތަފާސް / ދިރާސާ ތަފާސް ކުރާ ގޮތުގެ ތަފާސް ގެ 3 ގައި ބަޔާންކުރާ ގޮތަށް ތަފާސް ކުރާ ގޮތް
2.2.	ތަފާސް ކުރާ ފަރާތުގެ ތަފާސް ކުރާ ގޮތުގެ ކުރިން 2 ވ ދުވަހުގެ ކުރިން 2023 ފެब്രുവരി 12:00 ގެ ކުރިން tender@ncit.gov.mv ގަޑި. ތަފާސް ކުރާ ގޮތުގެ ލިޔުން ތަފާސް ކުރާ ގޮތުގެ ދަށުން ކުރެވޭ ފަރާތްތަކުގެ ލިސްޓު www.ncit.gov.mv ގައި 2023 ފެब്രുവരി 5 ވ ފުރިހަމަ ވަގުތު 1:30 ގައި ފާސްކޮށް ދައްކާ ގޮތުގެ ލިޔުން ހުށަހަޅާ ފަރާތްތަކުގެ ލިސްޓު ތަފާސް ކުރާ ގޮތުގެ ކުރިން ދައްކަންވާ ފައިސާ ދައްކާ ގޮތުގެ ލިޔުން ހުށަހަޅާ ފަރާތްތަކުގެ ލިސްޓު

ހުޅުވާނީ މިމަސައްކަތަށް އަންގާފައިވާ ހިސާބު ހުރަހައިފައިވާ ފާރާތްތަކުގެ ބެލުމުގައި ހާޒިރުވެވޭ ބޭސް ވެރިން ނުވަތަ ބޭސްވެރިންގެ ބަދަލުގައި އެފާރާތަކުން ކަނޑައަޅާ ފާރާތަކުގެ ހާޒިރުގައެވެ.	
ބޭސް ހުރަހެއްޓޭނެ ފާރާތަކަށް (ކޯލްޑްޗޭން ރެފްރިޖިރޭޓަރ) (ހ) ދިވެހިރާއްޖޭގައި ރަޖިސްޓަރީކޮށްފައިވާ ދިވެހި ވިޔަފާރިއަކަށްވުން. (ށ) މެޑިކަލް އިންޕޯޓް ރެޖިސްޓްރީގައި ރަޖިސްޓަރީވެފައިވާ ފާރާތަކަށްވުން. (ނ) އެސް.އެމް.އީ ގެ ގޮތުގައި ރަޖިސްޓަރީކުރެވިފައިވުން. (ރ) މި ބޭނުމާއި އެކު ހުރިހާ ޕްރޮޓޮކޯލްތަކާ އެއްގޮތަށް ފާރާތުގެ އޮފިސަރސްޓެ ރާޖޭއަކަށްވުން.	.2·3
ބޭސް ހުރަހެއްޓުމުގެ ތެރޭގައި، ވިޔަފާރީގެ ފާރާތުން އިދާރާއަށް ހާޒިރުވާ ފާރާތަކީ ބޭސްވެރި ގެއް އެންމެހައި ވިޔަފާރިއެއްގައި ސާއިންޓިފިކް، ބޭސް ހުރަހަށް ފާރާތުގެ ހުއްދަ ނުވަތަ ޕަރމިޓް އޮތް އެޖެންޓް ލިބިފައިވާ ފާރާތެއްކަމުގައި ބެލެވޭނެއެވެ.	.2·4
ކޯލްޑްޗޭން ރެފްރިޖިރޭޓަރގައި ހިފެހެއްޓުމާ ކަންތައްތަށް ފުރިހަމަ ނުވާ ބޭންސްތައް ބާލާފައިވާނެއެވެ. އަދި މި ބޭންސްތައް އިތުރުކުރުން މަނިޓަރިކުރުމާ ނުގެންދާވާނެއެވެ.	.2·5
ބޭސް ހުރަހެއްޓުން ކަނޑައަޅާފައިވާ ސްޓޯރޭޖް ހަމަޖެހިފައިވާ ހުރަހާ ބޭސްތަކެއް ބަލަހައްޓަން ނުޖެހޭނެއެވެ.	.2·6
ބޭސްފިރިން ހުރަހާ ޓެމްޕަރޭޗަރ ހުރިހާނާތުގެ ތެރޭގައި ބަހައްޓަން ކަނޑައަޅާފައިވާ ގޮތުގެ. (ހ) ޓެމްޕަރޭޗަރގެ ކޮންމެ ސަރުކާރުގައި ނަންބަރު ޖަހާފައި ހުރިހާނާ ވާނެއެވެ. (ށ) ޓެމްޕަރޭޗަރ ހުރިހާނާތުގެ ބައިންޓް ކަނޑަވާނެއެވެ. (ނ) މި ޓޭބަލް ސްޓޭޝަން 4 ގައި ބަޔާންކުރާ ހުރިހާ ތަކެތި ހަމަޖެހިފައިވާނެއެވެ.	.2·7
ބޭސް ހުރަހަޅަންވާނީ ބަންދުކުރެވިފައިވާ ސިޓީއުތަކެއްގައެވެ. އަދި ސިޓީއުތަކުގެ ބޭރުގައި މި ދަންނަވާ މައުލޫމާތު ހިމަނަންވާނެއެވެ. (ހ) ބޭސްގެ ނަން (ށ) އިއުލާން ނަންބަރު (ނ) ހުރަހާ ފާރާތުގެ ނަން	.2·8
ޓެމްޕަރޭޗަރގައި ހިފޭ ކަންކަމާއި ގުޅޭގޮތުން އިތުރުކުރުން މަނިޓަރިގައި އިތުރަށް ސާފުކުރުމަށް ބަންދުވާ މައުލޫމާތު ލިބިގަތުން ކުރުމުގެ އިޝްތިހާރު އިދާރާއަށް ލިބިދެންވާނެއެވެ. އަދި އިދާރާއިން ބަލާ މަސައްކަތުގައި ލިބިގަންނަ ހުރަހަގަތިޔަތަ، ބޭސް ކަނޑަލާ ކުރުމުގެ އިޝްތިހާރު އިދާރާއަށް ލިބިދެންވާނެއެވެ.	.2·9
ހުރަހާ ބޭސްގެ ބޭރު ވެއްޓޭ ޕީރިޔަޑު ދުވަސްވަނީ މުއްދަތެއް ރަނގަޅު ބަންދު ދުވަސްތަކަށް ނުހިމަނައި 90 (ނުވަދިހަ) ދުވަހެވެ.	.2·10
މިމަސައްކަތް ހަވާލުކުރެވޭ ފާރާތް ހޮވުމުގައި ބެލޭވާ އިތުރުކުރުން ކުރިއަށްދިޔަ ގޮއި އެއްގޮތަށް ވާހަކަ ދެއްކުން، އަދި މަޝްވަރާ ވާހަކަ ފާރާތަކާއެވެ.	.2·11
ބޭސް ހަވާލުވާ ފާރާތުގެ އަގަށް ހަމަޖެހޭ އަންގާނެއެވެ.	.2·12
ބޭސް ހަވާލުވާ ފާރާތް ކަނޑައެޅުމުގައި ކޮންޓްރެކްޓް ހަވާލުކުރުމުގެ ހުރިން، ބޭރުގައި ބައިވެރިވި ހުރިހާ ފާރާތްތަކަށް، އެބޭސް ހަވާލުވާ ކޮންޓްރެކްޓް ކަމާއި، ހަވާލުވާ ނުވާ ފާރާތްތަކާ ކޮބައިކަން އަންގާނެއެވެ. އަދި ބޭސް ހަވާލުވާ ނުވާ ފާރާތަކުން ބޭރުގައި ގޮތުން ހުށަހެޅޭ މައުލޫމާތު ލިބުމަށް، އެމައްސަލަ ހުށަހެޅުމަށް 5 (ފަހެއް) ދުވަހުގެ މުއްދަތެއް ދެވޭނެއެވެ.	.2·13

2.14.	ބީލަން ކާމިޔާބު ކުރިފަރާތުން ހުށަހެޅި ބިޑުގެ އަގު -/500,000ރ (ފަސްލައްކަ) ރުފިޔާއަށް ވުރެ އަގުބޮޑުނަމަ ބިޑު އެވޯޑްވާ ފަރާތުން އެގްރީމެންޓްގައި ސޮއިކުރުމުގެ ކުރިން މާލިއްޔަތު ޤަވާއިދުގައިވާގޮތަށް އެއްބަސްވުމުގައި ސޮއިކުރުމަށް ވަޑައިގަންނަވާއިރު ދިވެހިރާއްޖޭގައި ރަޖިސްޓްރީކުރެވިފައިވާ މާލީ ޚިދުމަތްދޭ ފަރާތަކުން ދޫކުރެވިފައިވާ ޕަރފޯމަންސް ގެރެންޓީގެ ގޮތުގައި ކަރާރުގެ އަގުގެ 7% ހަތެއް އިންސައްތަ އަދަދާ 51,788/25ރ (ފަންސާސްއެއްހާސް ހަތްސަތޭކަ އަށްޑިހައަށްރުފިޔާ / ފަންސަވީސް ލާރި) ހުށަހަޅަންވާނެއެވެ.
2.15.	މަސައްކަތުގެ މުއްދަތު ގުނަންފަށާނީ މަސައްކަތް ކުރުމަށް އެގްރީމަންޓްގައި ބަޔާންކޮށްފައިވާ ތާރީޚުން ފެށިގެންނެވެ.
2.16.	އެއްބަސްވުމުގެ ޢާންމު މުއްދަތަށް އަދި ޚާއްސަ މުއްދަތަށް މިފޮތުގެ ސެކްޝަން 6 ގައި ބަޔާންކޮށްފައި ވާނެއެވެ.

ސެކްޝަން 3.	ހޯދަންބޭނުންވާ ތަކެތި ނުވަތަ ޚިދުމަތުގެ މަޢުލޫމާތު
3.1.	ހުށަހަޅާތަކެއްޗަކީ ބަޔާންކޮށްފައިވާ ސްޕެސިފިކޭޝަނާ ދަށް ސްޕެސިފިކޭޝަނަކަށް ވެގެން ނުވާނެއެވެ.
3.2.	ތަކެތި ޑެލިވަރ ކުރަންޖެހޭނީ، ހުށަހަޅާފައިވާ މުއްދަތުގެ ތެރޭގައި، ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ، ކަލާފާނު ހިނގުން، މާލެ އަށް ރަސްމީ ބަންދު ދުވަސްތަކެއްނޫން ދުވަހަކު 14:00 ގެ ކުރިންނެވެ.
3.3.	ފައިސާ ދޫކުރާނީ، ސިސްޓަމް ބަލާ ޗެކުކުރުމަށްފަހު ތަކެތީގައި އެއްވެސް މައްސަލައެއް ނުވާކަމުގައި ވާނަމައެވެ.
3.4.	ތަކެތީގެ ސްޕެސިފިކޭޝަން އަދި އެހެނިހެން މައުލޫމާތު މި ސެކްޝަންގައި ބަޔާންކުރެވިފައިވާނެއެވެ.

#	Requirement
1	**01 Nos x Remote Access Concentrator Firewall**
	General Requirement (Appliance And OEM)
	Make and Model of the proposed firewall should be clearly stated
	OEM of the proposed firewall should be in “Leaders” quadrant as per the latest 5 years Gartner report for Enterprise firewalls
	OEM of the proposed firewall should have an ICSA certification for Antivirus, IPS, firewall, IPSec and SSL VPN technologies
	Should be an appliance-based hardware platform which is optimized and purpose-built for high performance with a security-hardened, purpose-built operating system
	Should have enterprise license for firewall, VPN (IPsec & SSL), etc. User/IP/Host based license are not accepted
	Should use hardware acceleration to optimize packet encryption/decryption and application-level content processing
	Should include redundant hot-swappable power supply units
	Should be 19” rack mountable
	Interface and Connectivity Requirements
	Should support SD-WAN architecture without any additional module, license upgrade or hardware upgrade

	Proposed firewall should have the following interfaces • 4 x 25GE SFP28 interfaces • 4 x 10GE SFP+ interfaces • 16 x 10/100/1000 RJ-45 Copper Interfaces • 8 x 1GE SFP interfaces • 1 x Dedicated RJ-45 MGMT interface 1 x Dedicated RJ-45 HA interface
	Should Come With 4 x 10GE SFP+ Multi-Mode (SR) transceivers (Compatible with The Proposed Appliance)
	Performance Requirements
	Should support at least 8 million concurrent connections
	Should support a minimum of 550,000 new sessions per second processing
	Should have following minimum performance based on real-world Traffic Mix: • NGFW Throughput - 11 Gbps • IPS Throughput - 14 Gbps • Threat Prevention Throughput - 10 Gbps SSL Inspection Throughput - 9 Gbps
	Network and Routing Requirements (Should Support the Following)
	Should Support Static Routing
	Should Support Policy-based Routing
	Should Support Dynamic Routing (RIP, OSPF, BGP &IS-IS) for both IPv4 and IPv6
	Should Support Multicast Routing
	Should Support Net Flow or sFlow
	Should Support Application Aware Routing
	Additional Network Requirements (Should Support the Following)
	Should Operate in standard NAT mode, or transparent mode
	Should Support NAT functionality (including PAT)
	Should Support Policy-based NAT
	Should Support User-Group have based Authentication (Identity based firewalling) and Scheduling
	Should Support Device have based and OS based policies
	Should Support IPv6 for both NAT and Transparent Mode
	Should Support Creation of up to 10 virtual firewalls on the device itself. (Any required licenses should be included in the proposal.)
	Authentication Requirements
	Support for authentication at the firewall policy level
	Support for external RADIUS, LDAP and TACACS + integration for User and Administrator Authentication
	Support for Native Windows Active Directory Integration
	Support PKI/Digital Certificate based two-factor Authentication for Administrators
	Administration & Management Requirements
	Support WebUI (HTTP/HTTPS) and CLI (Telnet/ SSH) based management
	Configurable options to define remote access to the firewall on any interface and restrict the same to a specific IP/Subnet (i.e., Trusted Hosts for Management)
	Support connecting directly to the firewall through a console connection (RJ45 or DB9)
	Should Support SNMPv2c and SNMPv3
	Support generating to generate automatic notification of events via mails/syslog
	Able to provision to send alerts to multiple email recipients
	Support for role-based administration of the device
	Concurrent login for multiple Administrators
	Customizable Dashboard and Widgets
	Provide A Method to export the device rule set and configuration to a text file via Web or TFTP
	Support for image upgrade via FTP, TFTP and WebUI

	Support system software rollback to the previous version during upgrade
	Encryption & VPN Requirements
	Should Consist of integrated VPN that minimally support the following protocols DES, 3DES,MD5,SHA-1, SHA-256, MD5, Diffie-Hellman Group1, Group2,Group 5, IKE v1/2, AES 128/192/256
	Support Hub and Spoke VPN topology
	IPSec VPN shall support XAuth over RADIUS and RSA SecurID
	Should have integrated SSL VPN with no user license slab restriction
	Support SSL two-factor authentication with Digital Certificates, or Hardware/Mobile tokens
	Support Single Sign-On Bookmarks for SSL Web VPN
	Support Windows, Linux and MAC OS for SSL-VPN.
	Support NAT within IPsec/SSL VPN tunnels
	Support PPTP and L2TP over IPsec VPN protocols
	IPS and Application Control Requirements
	Should Have built-in Signature and Anomaly based IPS engine on the same appliance
	Should Have Means Of mitigation of denial of Service and Buffer Overflow Attacks
	Should Have an IPS Certified by an independent certification/testing body such as NSS Labs and ICSA
	Should be Able to identify and control applications
	Should be Able to control popular IM/P2P, social media, malware, applications regardless of port/protocol
	Should be Able to control cloud-based applications and should able to route the specific applications via different WAN links based on the jitter and latency on the link
	Gateway Antivirus
	Should facilitate embedded gateway antivirus support
	Should include anti-spyware and worm prevention
	The facilitated antivirus should support real-time detection of viruses and malicious code for HTTP,HTTPS, FTP,SMTP, SMTPS,POP3, IMAP, NNTP and IM
	Should have configurable policy options to select what traffic that are scanned for viruses
	Should have options to prevent user downloads based on file extension as well as file type
	Should have support for Flow-Based Antivirus Scanning Mode
	Should be capable of scanning Encrypted VPN tunnel traffic originating from the client for virus
	Should have the ability of antivirus scanning for IPv6 traffic
	Should be able to Integrate with Advanced Threat Prevention solution for zero-day threat mitigation
	Web Content Filtering Requirements
	Should facilitate embedded web content filtering feature
	Web content filtering Should work independently without the need to integrate with an external proxy server
	Web content filtering should have the facility to block URLs based on categories
	Web content filtering should support HTTP and HTTPS traffic
	Should be able to block URLs hosting spywares/adware etc.
	Should be able to block different categories/sites based on User Authentication
	Should have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable
	Should have options to customize the “Blocked Webpage Message” information displayed to end users
	Should be able to Integrate with an Advanced Threat Prevention solution to prevent from zero-day threats in unknown web URLs
	Should be able to detect DNS-based spoofing attacks
	Should be able to assign usage-based and time-based quota for bandwidth web categories
	Should include DNS filtering feature to block DNS requests to known botnet C&C domains
	Should support category-based DNS filtering

	Should support safe search for DNS requests. This feature should be supported for Google and YouTube.
	High availability Requirements
	Should support Active-Active as well as Active-Passive redundancy architecture
	Automation
	Should include automation capabilities in order to take automated action based on defined triggers and the automation should be able to trigger based on specific log events, CPU/Memory high incidents, license expiry, compromised host detection and HA failover.
	Automation actions should include running CLI scripts, email/MS teams notifications and Quarantine of endpoints.
	In response to a trigger, multiple automation actions should be supported to be carried out in parallel or sequentially
	If a CLI script is run to collect diagnostic information from the firewall in response to a trigger, the email notification action should be able to attach the output of the CLI script to the email body.
	Other Requirements
	Should Support Jumbo Frames
	Should have option to configure traffic shaping on policy basis, application basis and IP basis. It shall have provision to define guaranteed bandwidth and maximum bandwidth
	Vendor/Supplier Eligibilities
	Vendor shall operate 24/7/365 global Technical Assistance Center (TAC) with telephone and e-mail support.
	Bid Submitter Should be authorized by the original manufacturer and submit the Original Manufacture's Authorization Certificate along with the bid
	Warranty and Security Subscriptions
	The proposed firewall should have OEM authorized warranty / support services (TAC) for 24x7 for at least One (01) year
	The proposed firewall should minimally include 1-Year security subscription with IPS, Advanced Malware Protection, Application Control, Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and Cloud Sandbox Service
2	**16 Nos x Remote Branch Firewall**
	General Requirements
	Make and Model of the proposed firewall should be clearly stated
	OEM of the proposed device should be in "Leaders" quadrant as per the latest 2 years Gartner report for WAN edge infrastructure
	OEM of the proposed device should be in "Leaders" quadrant as per the latest 2 years Gartner report for Enterprise firewalls
	OEM of the proposed device should have ICSA certification for Antivirus, IPS, firewall, IPsec and SSL VPN technologies
	Should be an appliance-based hardware platform which is optimized and purpose-built for high performance with a security-hardened, purpose-built operating system
	Should have enterprise license for firewall, VPN (IPsec & SSL), etc. User/IP/Host based license are not accepted
	Should use hardware acceleration to optimize packet encryption/decryption and application-level content processing
	Interface and Connectivity Requirements
	Should have USB interfaces for backing up/ restoring configuration, upgrading software images and connecting 3G/4G modems
	Should support SD-WAN architecture without any additional module or hardware upgrade
	Proposed device shall have the following interfaces • 5 x 10/100/1000 RJ-45 Copper Interfaces • 1 x USB interface 1 x RJ-45 console interface
	Performance Requirements

	Should support at least 700,000 concurrent connections
	Should support a minimum of 35,000 new sessions per second processing
	Should support data throughput of a minimum 5 Gbps
	Should have following minimum performance based on real-world Traffic Mix • NGFW Throughput - 800 Mbps • IPS Throughput - 1 Gbps • Threat Prevention Throughput - 600 Mbps SSL Inspection Throughput - 300 Mbps
	Network & Routing Requirements
	Should support Static Routing
	Should support Policy-based Routing
	Should support Dynamic Routing (RIP, OSPF, BGP &IS-IS) for both IPv4 and IPv6
	Should support Multicast Routing
	Should support Net Flow or sFlow
	Should support Application aware Routing
	Features Requirements
	Should be able to operate in standard NAT mode, bridge mode or transparent mode
	Should provide NAT functionality, including PAT
	Should support Policy-based NAT
	Should support User-Group based Authentication
	Should support device based and OS based policies
	Should have IPv6 support for both NAT and Transparent Mode
	Should support the creation of up to 10 virtual instances on the device itself. Any required licenses should be included.
	Authentication Requirements
	Should have support for authentication at the firewall policy level
	Should have support for external RADIUS, LDAP and TACACS + integration for User and Administrator Authentication
	Should support for Native Windows Active Directory Integration
	Should support PKI/Digital Certificate based two-factor Authentication for Administrators
	Administration & Management Requirements
	Should support WebUI (HTTP/HTTPS) and CLI (Telnet/ SSH) based management
	Should have configurable options to define remote access to the device on any interface and restrict the same to a specific IP/Subnet (i.e., Trusted Hosts for Management)
	Should support connecting directly to the device through a console connection (RJ45 or DB9)
	Should Support have SNMPv2c and SNMPv3
	Should Be Able to generate automatic notification of events via mails/syslog
	Should be able to send alerts to multiple email recipients
	Should support role-based administration of the device
	Should support simultaneous login of multiple Administrators
	Should have provision to customize the dashboard by selecting suitable Widgets etc.
	Should provide a means for exporting the device rule set and configuration to a text file via Web or TFTP
	Should support for image upgrade via FTP, TFTP and WebUI
	Should support system software rollback to the previous version during upgrade
	Encryption & VPN Requirements
	Should have integrated VPN that support the following protocols DES, 3DES,MD5,SHA-1, SHA-256, MD5, Diffie-Hellman Group1, Group2,Group 5, IKE v1/2, AES 128/192/256
	Should support hub and spoke VPN topology
	IPSec VPN shall support XAuth over RADIUS and RSA SecurID
	Should have integrated SSL VPN with no user license slab restriction
	Should support SSL two-factor authentication with Digital Certificates, or Hardware/Mobile tokens

	Should support Single Sign-On Bookmarks for SSL Web VPN
	Should support Windows, Linux and MAC OS for SSL-VPN. (Shall have always-on clients for the said OSs apart from browser based access.)
	Should support NAT within IPSec/SSL VPN tunnels
	Should support PPTP and L2TP over IPSec VPN protocols
	SD WAN Support
	Should Support redundant links with active/active traffic load balancing
	Should Support for multiple WAN link types (4G LTE, Fiber, MPLS, ILL, etc.)
	Should Support Encryption of the WAN transport
	Monitor the quality of the WAN links (packet loss, jitter and delay) and support for creating Service Level Agreements (SLA) based on the monitored statistics
	Support Forward Error Correction (FEC) and packet duplication as WAN remediation techniques
	Should provide a method for providing direct branch to branch WAN connectivity
	User/User-group based traffic steering should be available to be implemented for SD-WAN policies.
	Application based traffic steering should be available to be implemented for SD-WAN policies. Applications should be selectable by specifically by name in the SD-WAN policies.
	SD-WAN policies should provide multiple WAN strategy options. Minimally • Should Be Able to Manually assign WAN link to an application/Internet service • Should Be Able to Assign the best quality WAN link as per the measured performance (based on packet loss, jitter, latency, bandwidth or a custom profile) to an application/Internet service Should Be Able to Assign the WAN link with the lowest SLA target to an application/Internet service Should be Able to Load balance traffic across all WAN links that meet the SLA targets
	IPS and Application Control Requirements
	Should have built-in Signature and Anomaly based IPS engine on the same unit
	Should be able to mitigate denial of service attacks
	Should be able to mitigate buffer overflow attacks
	Proposed device should have an IPS Certified by an independent certification/testing body such as NSS Labs and ICSA
	Should identify and control applications
	Should be able to control popular IM/P2P, social media, malware, applications regardless of port/protocol
	Should be able to control cloud-based applications and should able to route the specific applications via different WAN links based on the jitter and latency on the link
	Gateway Antivirus
	Should facilitate embedded gateway antivirus support
	Should include anti-spyware and worm prevention
	The Facilitated Gateway antivirus Should support real-time detection of viruses and malicious code for HTTP, HTTPS, FTP,SMTP, SMTPS,POP3, IMAP, NNTP and IM
	Should have configurable policy options to select what traffic to scan for viruses
	Should have options to prevent user downloads based on file extension as well as file type
	Should have support for Flow-Based Antivirus Scanning Mode
	Should be capable of scanning Encrypted VPN tunnel traffic originating from the client for virus
	Should have the ability of antivirus scanning for IPv6 traffic
	Should be able to Integrate with Advanced Threat Prevention solution for zero-day threat mitigation
	Should have an endpoint client that can co-exist with any antivirus solution and provide zero-day threat mitigation integration with Advanced Threat Prevention solution. Client should be able to identify the vulnerabilities on the endpoints
	Web Content Filtering Requirements
	Should facilitate embedded web content filtering feature
	Should work independently without the need to integrate with an external proxy server

	Should have the facility to block URLs based on categories
	Web content filtering should support HTTP and HTTPS based traffic
	Should be able to block URLs hosting spywares/adware etc
	Should be able to block different categories/sites based on User Authentication
	Should have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable
	Should have options to customize the “Blocked Webpage Message” information displayed to end users
	Should be able to Integrate with an Advanced Threat Prevention solution to prevent from zero-day threats in unknown web URLs
	Should be able to detect DNS-based spoofing attacks
	Should be able to assign usage-based and time-based quota for bandwidth web categories
	Should include DNS filtering feature to block DNS requests to known botnet C&C domains
	Proposed device shall support category based DNS filtering
	Proposed device shall support safe search for DNS requests. This feature should be supported for Google and YouTube.
	Automation
	Should include automation capabilities in order to take automated action based on defined triggers and the automation should be able to trigger based on specific log events, CPU/Memory high incidents, license expiry, compromised host detection.
	The automation actions should include running CLI scripts, email/MS teams notifications and Quarantine of endpoints.
	In response to a trigger, multiple automation actions should be supported to be carried out in parallel or sequentially
	If a CLI script is run to collect diagnostic information from the device in response to a trigger, the email notification action should be able to attach the output of the CLI script to the email body.
	Other Requirements
	Should Support Jumbo Frames
	Should Be Able To configure traffic shaping on policy basis, application basis and IP basis. It shall have provision to define guaranteed bandwidth and maximum bandwidth
	Should support packet capture/sniffer to capture and examine the contents of individual data packets that traverse the device
	Vendor/Supplier Eligibilities
	Vendor shall operate 24/7/365 global Technical Assistance Center (TAC) with telephone and e-mail support.
	Bid Submitter Should be authorized by the original manufacturer and submit the Original Manufacture’s Authorization Certificate along with the bid
	Warranty & Subscriptions
	The proposed firewall should have OEM authorized warranty / support services (TAC) for 24x7 for at least One (01) year
	The proposed firewall should minimally include 1-Year security subscription with IPS, Advanced Malware Protection, Application Control, Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and Cloud Sandbox Service
3	**01 Nos x Centralized Management Appliance**
	The SD WAN Solution should have a centralized management appliance for managing a minimum 20 firewall appliances of the same OEM from a single console. The centralized Management Solution Should Be of a Virtual Appliance
	The proposed virtual appliance should support the following virtualization platforms at a minimum • VMware ESX/ESXi • Microsoft Hyper-V • Citrix XenServer, KVM • Amazon Web Services (AWS) Microsoft Azure
	Should provide the ability to collectively configure the device settings, objects and policies across all the firewalls from a single user interface

	Should provide the ability to review, approve and audit policy changes from a central console
	Should support automated process to facilitate policy compliance and policy lifecycle management
	Should support enforcing workflow to reduce risk for policy and configurations changes
	Should support providing security updates for all managed devices from the management solution itself.
	Should Provide and Support A RESTful API which allows to create customized, branded web portals for policy and object administration
	Should provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert(s) to administrator defined e-mail address(es)
	Should provide the ability to create multiple subaccounts or virtualized sub accounts with each account having its own administrators/users with access/views to only their respective devices.
	Should have the capability to maintain audit trail (history) of all configuration changes. These different versions should be comparable to each other to identify differences. The solution should also provide the ability to restore to previous configuration versions.
	Should provide the operational status, performance data and firmware information of all managed devices.
	Should provide monitoring capabilities for the managed device SD-WAN features.
	Policy creation, management and application of policies.
	Support for firmware Management/upgrades for the managed devices from a central console
	Should Provide traffic and performance statistics of the Managed Devices
	Should Support certificate management for all the managed devices
	Should support Zero-touch provisioning (ZTP) for provisioning managed devices, when new Devices are being deployed in remote locations with minimum intervention of an on-site technical personnel
	The Management Solution should function in a manner that failure of the Management solution Should not impact the managed devices traffic flow
	The management solution should be able to fetch the configurations from the managed devices and rebuild the management database in case of complete data loss of the management appliance.
	Should include a central log retention capability to receive logs from all the managed firewall devices.
	Role Based Access Control (RBAC) should be supported for granting different authorization levels to different administrators in a granular manner
	Vendor/Supplier Eligibilities
	Vendor shall operate 24/7/365 global Technical Assistance Center (TAC) with telephone and e-mail support.
	Bid Submitter Should be authorized by the original manufacturer and submit the Original Manufacture’s Authorization Certificate along with the bid
	Warranty & Subscriptions
	The proposed solution should have OEM authorized warranty / support services (TAC) for 24x7 for at least One (01) year
4	**01 Nos x Centralized Logging and Reporting**
	Logging and Reporting Solution should be an out of the box solution. Should be proposed as a virtual appliance
	Proposed virtual appliance should be capable of handling a minimum 5GB of logs per day.
	The solution should provide with threat feed subscription for identifying comprised hosts along with automation incident response actions.
	Logging and Reporting solution should support to integrate multiple devices (From the Same Brand) and should provide the ability to create multiple virtualized subaccounts with each account having its own administrators/users with access to only their respective firewalls.
	Should be able to view the current session details from the dashboard, including, Source, Destination, Country, Application, etc.
	The proposed solution Should include a central log retention for all the appliances added to it from the same OEM solution.

	The proposed solution should be able to integrate with Incident management systems, ticketing solutions and should be able to generate events based on the configured handlers and accordingly send email alerts to intended recipients.
	Should include inherited log archiving capabilities and should be able to customize according to the Administrators requirement.
	The complete traffic and system event logs should be retained in the logging solution
	Should be able to Archive logs after the defined analytics retainment period and should be able to export and import back for analytics to and from to an external backup.
	Should provide administrator authentication via TACAS/RADIUS/LDAP and should support role-based access management.
	The solution should support alerting notifications through SNMP traps, email, and remote syslog.
	The Reporting capabilities should not be limited to templates or predefined formats based on the administrator's requirement. Also, it should be able to create custom reports.
	Should support out of the box Management reports for NGFW and should be able to create any new reports based on custom database queries.
	Should support to generate the following customized reports for daily, weekly, monthly, yearly etc., and but not limited to link bandwidth utilization, device health monitors, security enforcements, system logins.
	Should provide the ability to schedule reports to run at non-peak hours or run-on demand. Should be able to send the reports to intended recipients via email.
	All reports must be exportable in PDF, HTML and CSV formats.
	Vendor/Supplier Eligibilities
	Vendor shall operate 24/7/365 global Technical Assistance Center (TAC) with telephone and e-mail support.
	Bid Submitter Should be authorized by the original manufacturer and submit the Original Manufacture's Authorization Certificate along with the bid
	Warranty & Subscriptions
	The proposed central management solution shall have OEM authorized warranty / support services (TAC) for 24x7 for One (01) year
5	**Installation, Configuration, Migration and Training**
	Hardware installation including mounting, management cabling and power up as per manufacturer guideline
	The vendor MUST have at minimum the following full time OEM Certified Professional/Engineer under its payroll to provide installation, configuration, integration, migration and training services. All relevant engineer(s) certificates and supporting documents shall be included with the proposal. Primary required certificates of the engineer(s): •Cisco CCNA Certified for Routing and Switching Certified •Cisco CCNA and CCNP Certified for Security Certified •OEM Certified for the Proposed Firewall
	Perform site readiness assessment ensuring hardware environment is ready for project commencement
	Identify and assess existing environment including network security devices, core network switching and routing devices.
	Ensure current deployment and configuration is setup such that the configuration and migration works can be conducted with minimal downtime.
	Shall provide planning, deployment and user acceptance test details
	The devices and appliances shall be installed and configured as per manufacturer best practice guidelines and as per industry best practices.
	Upgrade to the latest release of stable firmware and confirm it is at a supported and appropriate version.
	Configure secure management console for all devices and appliances.
	Install or register any license keys for the purchased
	Design appropriate LAN,WAN, and DMZ security policies.
	Configure application control policies
	Configure AV and Web filtering policies

	Configure antispam filtering
	Configure IPS policies
	Configure traffic shaping and ISP WAN load balancing
	Network segmentation and configure appropriate security policy per segment
	Configure remote access connectivity policies
	Configure centralized management appliance as per industry best practice
	Configure centralized logging and reporting appliance and standard security reporting
	On the job training for up to 02 technical person on Install, configure, manage and troubleshoot the Storage system and its components
	Comprehensive testing and a detailed documentation on the configuration and settings of the delivered solution shall be provided.
6	**Service Level Expectations** **a)** The support service vendor should provide the contact number of a single point of contact to facilitate immediate contact by client's representative and he or she shall be responsible to liaise with all vendors for rectification of faults within the Next Business Day. **b)** Defective equipment shall be replaced by the bidder at his own cost including the cost of transport if any; **c)** The support service vendor shall provide all normal toolkit and test equipment needed for the maintenance of the hardware to the engineer. **d)** System maintenance and support services will include the following activities. ✓ 24 x 7 on-line Support. ✓ Patch updating and major / minor software version upgrading support. ✓ Phone/Email TAC support must be provided during support period ✓ Issue resolution / Onsite Visits within 1 hour of hardware failures reported Local TAC support plan must be maintaining by the Bidder for the maintenance period.
7	**Maintenance Support Services including on-site Technical Support:** • On-site hardware repair/replace and maintenance support service should be delivered by experienced OEM Certified Engineer • On-site diagnostics and repair service should be delivered by experienced OEM Certified Engineer and should diagnose, repair, and test the unit to ensure optimal performance. • Technical support experienced engineers should be available to answer our questions, giving us peace of mind knowing the help we need is there when we need it • Flexible on-site response times that best meets the business requirements • Service summary report should provide after each work performed including recommendations for service to ensure optimal performance • Maintenance Support Engineer should check and ensuring the unit is operating with the most recent firmware version. Firmware upgrades shall provide at no extra charge. • During each maintenance visit, field service Engineers should run tests to verify our system is functioning correctly in all operational modes, stopping problems before they start. • Maintenance Support Engineer should follow well-defined set of processes and procedures to be able to provide quality services, as per Industry standard. The support service vendor shall maintain critical parts locally in Male' to provide after sale support.
8	Warranty Minimum Duration Parts: 3 Year(s); Service: 3 Year(s) On-Site: 3 Year(s) with 24x7 on call assistance
9	Full Installation and initialization is required
10	Hands on training of the operations should be provided at the time of installation

ސެކްޝަން 4.	ބީލަން ހުށަހަޅާއިރު ތިރީގައިވާ މަޢުލޫމާތު އަދި ލިޔުންތައް ހުށަހަޅަންވާނެއެވެ.
.4.1	ހުށަހަޅާ މަޢުލޫމާތުގެ ޗެކްލިސްޓް
.4.2	ބީލަން ހުށަހަޅާފޯމު

4.3.	ގަބޫލުކުރާ ބޭނުންވާ ފައިލް ގިނަ / ދަތި ކަމުގައި ހިނގާ ކަންކަން
4.4.	ހުނަރާއ ގެނައުވާނެ، ގެނައުންތަކާ ގުޅޭ ތަފާތު ގަދަކަން ބަލާ ގޮތް
4.5.	ތަކެތި ހުއްދަ ގަނޑަށް (ދުނިޔެއަށް) ތ ހުރަތަކާ ގަދަތަކާ ދުއްވައިގެ ތަކެތި ގަނޑުވެ ދާ ގޮތް
4.6.	ތިލަނގާ ބަދަލު ކުރުން / ކެންސަލް ކުރުން / ކަނޑައެޅި ގަނޑުގެ ތެރެއިން ގަތުން / ވަކި ކުރުން)
4.7.	ހިއްސާ ދޫކުރުން ހުއްދަ ދިނުމާ ގުޅޭ ގޮތްތައް
4.8.	ހިއްސާ ދޫކުރުން ހުއްދަ ދިނުމާ ގުޅޭ ގޮތްތަކާ ގުޅޭ ކަންކަން ހިއްސާ ދޫކުރާ ކުންފުނި ތަކުގެ ލިބިފައިވާ ހައްގުތައް (ވޯޓު ލުއްވުމުގެ ހައްގު) - ހިއްސާ ގަނޑު ބަދަލު ކުރުން
4.9.	ލޯނު ހިންގުމަށް ބޭނުންވާ ގޮތްތަކާ ގުޅޭ ކަންކަން ބަލާ ގޮތް
4.10.	ލޯނު ހިންގުމަށް ބޭނުންވާ ގޮތްތަކާ ގުޅޭ ކަންކަން ބަލާ ގޮތް (ލޯނު ހުއްދަ ދިނުމާ ގުޅޭ ގޮތް)
4.11.	ލޯނު ހިންގުމަށް ބޭނުންވާ ގޮތްތަކާ ގުޅޭ ކަންކަން ބަލާ ގޮތް (ދުވަސް 03 ދަށު ރަނގަޅު)
4.12.	ދަށަނބަ ތަކެތި ބަދަލުކުރުން ފާސްކުރުމާ ގުޅޭ ގޮތް ބަލާ ގަނޑުގައި ހިނގާ ކަންކަން
4.13.	ފާސް ފުށުން ހިނގާ ގޮތް ބަލާ ގަނޑުގައި ހިނގާ ކަންކަން "ގަބޫލުކުރާ ކަންތައް ފުރިހަމަ ކުރުމަށް ދަށުގައި ބުނެފައިވާ ތަކެތި ހުށަހަޅާ ފަދަ ލިޔުންތަކާ ގުޅޭ ގޮތް 2019، 2020 ތަ 2021 ވަނަ ހަފްތާ ގަބޫލުކުރާ ކަންކަން ހުއްދަ ދިނުމުގެ ކުރިން ކުންފުނި ތަކުގެ ބަލައިގަތުމަށް ހުރި ގޮތް (ފަށާ ދުވަހުން 03 ގެ ކުރިން 03)
4.14.	ތ ބަލައިގަތުމަށް ހުރި ގޮތުގެ ގެ ގުޅުން ދިނުމަށް ކުރިން ކުންފުނި ތަކުގެ ބަލައިގަތުން ހުރި ގޮތް ގަބޫލުކުރާ ކަންކަން ދިވެހިރާއްޖެ ގައި ހުންނަ ކުންފުނި ތަކަށް 7,398/32 ރ (ހަމަޖެހުނު ތަކެތި ހުށަހެޅުމަށް ހުރި ގޮތް / ތަކެތި ދިރާގު) ގ ތ ބަލައިގަތުމަށް ހުރި ގޮތް ގުޅުން ދިނުމުގެ ގޮތް

ގ. ތަކެތި ހޯދުމުގެ ގޮތް		
ގުޅުން ދިނުމުގެ ގޮތް	**ގުޅުން ދެނެގަތުމުގެ ގޮތް**	**ގިނަކަން (100%)**
Price	$\frac{Lowest\ Proposed\ Price}{Proposed\ Price\ By\ Bidder}\ x\ 70$	70%
Experience	• 4 points for each reference letter / completion certificate signed and stamp by the client. • Each bidder will get maximum 20 points	20%
Delivery	$\frac{Lowest\ Propsed\ duration\ (in\ Days)}{Bidder's\ Proposed\ duration\ (in\ Days)}\ x\ 10$	10%

- މާލީ ޙިސާބުތަކަށް ވަޒަންކުރާނެ ގޮތް މި ފޯމުގެ 6.4 ގައިވާ ގޮތުގައި ބައްލަވާނެއެވެ.

ސެކްޝަން 6. ބިޑާއި އެކު ހުށަހަޅަން ޖެހޭ ލިޔުންތައް

- މި ސެކްޝަނގައި ބަޔާންކުރާ ލިޔުންތައް ޕްރޮޕޯޒަލްގައި ހުށަހަޅަންވާނެއެވެ.
- މި ލިޔުންތަކާއި އެކު ސަޕްލިމެންޓްގެ ޑޮކިއުމަންޓް ހުށަހަޅަން ބޭނުންވާނަމަ އެތަކެތި ފޮނުވަންވާނެއެވެ.
- މާލީ ޙިސާބުތަކަށް ބައްލަވާނީ، ފައިނޭންޝަލް ސްޓޭޓްމަންޓް ފޯމް، ނުވަތަ 2019، 2020 އަދި 2021 ވަނަ އަހަރުގެ ފައިނޭންޝަލް ސްޓޭޓްމަންޓްސް ނުވަތަ ކުންފުނީގެ އޮޑިޓް ރިޕޯޓް ކޮންމެ ކުންފުންޏެއް ހުށަހަޅަންވާނެއެވެ.
- ކުންފުނި އެކު ކޮންޓެކްޓް ސައިން، ބިޑް ޑޮކިއުމަންޓް އަދި ޕްރޮޕޯޒަލްގެ ޑޮކިއުމަންޓް ގެ ނަމޫނާ ހުށަހަޅަންވާނެއެވެ. މިގޮތުން ނަމޫނާގައި ހިމެނޭ މައުލޫމާތު ފުރިހަމަކޮށް ދިވެހިރާއްޖޭގައި ވިޔަފާރި ރަޖިސްޓްރީކޮށްފައިވާ މާލީ ހިސާބުތަކާ ފައިސާއާ ބެހޭ ދިނުން ބަލައިގަނެވޭނެއެވެ.
- ބިޑް ސެކިއުރިޓީ، ޕަރފޯމަންސް ގެރެންޓީ އަދި ކުއިން އޭޖެންޓް ކުންފުނި ބޭންކުން ލިބޭ ބަލައިގަނެވޭނެއެވެ.

6.1 ހުށަހަޅާ މައުލޫމާތުގެ ޗެކްލިސްޓް

بسم الله الرحمن الرحيم

ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ

National Centre for Information Technology

#	ހުށަހަޅާ ލިޔުންތައް	ސަފުހާ	ފާހަގަ
.1	ހުށަހަޅާ މައުލޫމާތުގެ ޗެކްލިސްޓް		
.2	ބިޑް ހުށަހަޅާ ފޯމު		
.3	ފައިނޭންޝަލް ބިޑްގެ އަގު ފޯމު / ނުވަތަ މި މައުލޫމާތު ހިމެނޭ ކޯޓޭޝަން		
.4	ހުށަހަޅާ ޕްރޮޖެކްޓްގެ ތަފްސީލް، ޕްރޮޖެކްޓް އުފެއްދި ފަރާތުން ތަޢާރަފްކުރާ މައުލޫމާތު، ޕްރޮޖެކްޓް ބްރޯޝަރ		
.5	ތަކެތި އުފައްދާ ފަރާތުން (މެނުފެކްޗަރަރ) ބިޑް ހުށަހަޅާ ފަރާތަށް ދޫކޮށްފައިވާ އޮތޯރައިޒްޑް ޑިސްޓްރިބިއުޓަރޝިޕްގެ ލިޔުން		
.6	ދިވެހިރާއްޖޭގައި ރަޖިސްޓްރީ ކުރެވިފައިވާ ވިޔަފާރިއަކަށްވާނަމަ. (ކުންފުނި / ޕާޓްނަރޝިޕް / ކޯޕަރޭޓިވް ސޮސައިޓީ / އަމިއްލަ ފަރުދުންގެ ރަޖިސްޓްރީގެ ކޮޕީ)		
.7	މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓުން ދޫކޮށްފައިވާ ވިޔަފާރީގެ ޕްރޮފައިލް ޝީޓް.		
.8	މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓްގައި ކުރި އަހަރު ފުރު ފަންޑީގެ ވިޔަފާރީގެ ދިންކިތަކުން ދިންމިއްސައިގައި ރަޖިސްޓްރީ ކުރެވިފައިވާ ދިވެހި ވިޔަފާރިއެއްކަން އަންގައިދޭ ސްޓޭޓަސް ލެޓަރގެ ކޮޕީ (އެސް.އެމް.އީ ރަޖިސްޓްރޭޝަން) - ރަޖިސްޓަރ ފޯމު ވެސް ފާހަގަކޮށްފައި		
.9	މޯލްޑިވްސް އިންލަންޑް ރެވެނިއު އޮތޯރިޓީން ދޫކޮށްފައިވާ ޖީއެސްޓީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓް ކޮޕީ		

.10	ފެންވަސް ތަކެއްޗާއި ގުޅޭ ކަންތައްތަކުގެ ދަށުގައި ކުރިއަށް ގެންދާ ކަންތައްތަކުގެ ތަފާސީލު (ފެ.ހުސް.ކަމަށް ކަނޑައެޅިފައިވާ)		
.11	ފެންވަސް ތަކެއްޗާއި ގުޅޭ ކަންތައްތަކުގެ ދަށުގައި ކުރިއަށް ގެންދާ ކަންތައްތަކުގެ ތަފާސީލު (ދުވަހުގެ 03 ގަސް ލަދުގަ)		
.12	ގަސްހާލަށް ބަދަލުގައި ހަރުގަނޑު ބަދަލުކުރުމުގެ ގަސްހާލަތް ކުރިއަށް ގެންދާ ތަފާސީލު		
.13	ފާރ ފުށުގައި ބަދި ގަނެވުމުގެ ހުށަހެޅުންތަކުގެ ތަފާސީލު "ގަތަށްޓަކާ ހިއްކުން" ގެންނަ ތަކެއްޗާ ދެކޮޅަށް ކުރެވިދާނެ ކަންތައްތަކާ ގުޅޭ ކަންތައްތަކުގެ ތަފާސީލު 2019، 2020 ތަކުގ 2021 ވަނަ ތަރަނދަ ގަތަށްޓަކާ ހިއްކުންތަކުގެ ތަފާސީލު ތަކުގައި ދިވެހިރާއްޖެ ފަރާތްތަކުން ހިއްކާ ތަކެއްޗާ ބެހެއްޓުމަށް ދެވޭ ބަދަލު (ދަށުގައި 03 ގ ގެ 03)		
.14	ތެދު ކަތަނގަ ތަކެއްޗާ ގ ދަތަނގަ ކަންތައްތަކުގެ ދަށުގައި ކުރިއަށް ގެންދާ ކަންތައްތަކުގެ ތަފާސީލު ގަތަށްޓަކާ ހިއްކުންތަކުގެ ދަށުގައި 7,398/32 ކ (ކަނޑައެޅި ތަކެއްޗާ ތަކެއްޗަށް ތަކެއްޗާ / ތަކެއްޗާ) ގ ތެދު ކަތަނގަ ތަކެއްޗާ ގުޅޭ ކަންތައްތަކުގެ ތަފާސީލު.		

6.2. ތަކެއްޗާ ގުޅޭ ގެންދާ ގެންދާ

بسم الله الرحمن الرحيم

National Centre for Information Technology

ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ

އިއުލާން ނަންބަރު:		ތާރީޚް	

ބީލަމާއި ގުޅުންހުރި ކަންކަމުގައި މުޢާމަލާތްކުރާނީ ސޮއި ކުރުމުގެ ހުއްދަ ދީފައިވާ ފަރާތުގެ	
ނަން:	
އައިޑީކާޑު ނަންބަރު	
މަޤާމު:	
ފޯނު ނަންބަރު:	
އީމެއިލް:	
ތާރީޚް:	
ސޮއި:	

މި ބީލަމުގައި ހުށަހަޅާފައިވާ ސަރުކާރުގެ ތަފްސީލުތަކާއި ކަމަށް އިޤްރާރުވަމެވެ. އަދި މަތީގައި ބަޔާން ކުރެވިފައިވާ ފަރާތަކީ ބީލަމާއި ގުޅިގެން މި ޢިދާރާއާއި ރަސްމީ ކޮންސަލްޓަންޓް ފަރާތްކަމާއި، ޢިދާރާއިގެ ފަރާތުން ބީލަމާއި ގުޅުންހުރި މުޢާމަލާތްތަކުގައި ސޮއިކުރުމުގެ ހުއްދަ ދީފައިވާ ފަރާތްކަމެވެ.

ބީލަން ހުށަހަޅާ ފަރާތުން (އަމިއްލަ ފަރުދެއް ނަމަ ވެރިފަރާތް، ކުންފުންޏެއް ނަމަ ޑިރެކްޓަރ އަދި ޕާޓްނަރޝިޕެއް ނަމަ މެނޭޖިންގ ޕާޓްނަރ) ސޮއިކުރައްވާނަމަ		
ނަން:		ތައްގަނޑު ސްޓޭމްޕް
މަޤާމު:		
ފޯނު ނަންބަރު:		
އީމެއިލް:		
ތާރީޚް:		
ސޮއި:		

6.3. ފައިނޭންޝަލް ޕްރޮޕޯޒަލް ފޯމު (ފިން ފޯމު-1) ނުވަތަ ފޯމުގައި ބަޔާންކޮށްފާ މަޢުލޫމާތު ހިމެނޭ ކޯޓޭޝަން. މި ފޯމު ނުވަތަ ކޯޓޭޝަނާއި އެކު، ތަކެތި އުފެއްދި ފެކްޓަރީން ދޫކޮށްފައިވާ ޕްރޮޑަކްޓް މަޢުލޫމާތު ހިމެނޭ ޑޮކް، ބްރޯޝަރ ތަކެތި ހުށަހަޅަންވާނެއެވެ. މި ފޯމުގެ ހުރިހާ މަޢުލޫމާތެއް ފުރިހަމަކުރަންވާނެއެވެ. ނުވަތަ ކޯޓޭޝަނުގައި ހިމަނަންވާނެއެވެ.

بسم الله الرحمن الرحيم

National Centre for Information Technology ނޭޝަނަލް ސެންޓަރ ފޯ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ

Reference No: (generated by the proponent)
Quotation validity: () days

#	Item / Equipment or work details	Qty	Price (MVR)	Total (MVR)
			Total	
			GST 8%	
			Warranty	
			Total with GST	

Bidder Stamp and Sign

____

6.4. ފަރާތްތަކުގެ ފައިނޭންސް ގުޅުން (ފޮށި ގުޅުން-2)

بسم الله الرحمن الرحيم

National Centre for Information Technology

ދާއިރާގެ ގޮތުގައި ކުރިއަށް ގެންދާ ކަންތައްތަކާ ގުޅޭ

Financial Data for Previous 03 Years [MVR Equivalent]			
Financial Information of the Year	**2019**	**2020**	**2021**
Information from Balance Sheet			
Total Assets			
Total Liabilities			
Net Worth			
Current Assets			
Current Liabilities			
Working Capital			
Information from Income Statement			
Total Revenues			
Profits Before Taxes			
Profits After Taxes			

- Attached are copies of financial statement (balance sheets including all related notes, and income statements), as indicated above, complying with the following conditions.
- All such documents reflect the financial situation of the Bidder.
- Historic financial statement must be complete, including all notes to the financial statements.
- Historic financial statements must correspond to accounting periods.

Evaluation criteria

Financial Situation evaluation

A. To be eligible the financial statements of the bidding party must show, average annual turnover of MVR 740,000.00 for the years 2019, 2020 and 2021.
(or)

B. To be eligible the financial statements of the bidding party must show, Minimum value of MVR 740,000.00 of the proposed price, for liquid asset, for the year 2019, 2020 and 2021.
(or)

C. If bidding party is unable to meet any of the above requirement they shall submit "Line of Credit Letter" as per the template in Form FIN – 3. (credit limit shall be no less than MVR 740,000.00 of the proposed price)

Bidder Stamp and Sign

_____

6.5. ފަރާތް ތެރޭ ކުށްވެ ހިނގާ ހާލަތު

[letterhead of the Bank/Financing Institution/Supplier]

[date]

To: *[Name and address of the Contractor]*

Dear,

You have requested {name of the bank/financing institution/supplier issuing the letter) to establish a line of credit for the purpose of executing {insert Name and identification of Project}.

We hereby undertake to establish a line of credit for the aforementioned purpose, in the amount of {insert amount}, effective upon receipt of evidence that you have been selected as successful bidder.

This line of credit will be valid through the duration of the contract awarded to you.

Authorized Signature:
Name and Title of Signatory:
Name of Agency:

6.6 ބިޑް ސެކިއުރިޓީގެ ނަމޫނާ

Form of Bid Security (Bank Guarantee)

WHEREAS, ………………………………………………..*[name of Bidder]* (hereinafter called "the Bidder") has submitted his Bid for the Project no……….issued by National Centre for Information Technology ……………………………… …………..for construction of …………………………… …….*[name of Contract]* (hereinafter called "the Bid").

KNOW ALL PEOPLE by these presents that We ………………………………………. *[name of Bank]* of ……… …………………… *[name of country]* having our registered office at ……………………………………………………………………………….. (hereinafter called "the Bank") are bound unto …………………………….*[name of Purchaser]* (hereinafter called "the Purchaser") in the sum of *……………………………………….. for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors, and assigns by these presents.

SEALED with the Common Seal of the said Bank this ……..day of …………….20……………..

THE CONDITIONS of this obligation are:

(1) If, after Bid opening, the Bidder withdraws his Bid during the period of Bid validity specified in the Form of Bid;

or

(2) If the Bidder having been notified of the acceptance of his Bid by the Purchaser during the period of Bid validity:

(a) fails or refuses to execute the Form of Agreement in accordance with the Instructions to Bidders, if required; or

(b) fails or refuses to furnish the Performance Security, in accordance with the Instruction to Bidders; or

(c) does not accept the correction of the Bid Price pursuant to Clause 27,

* The Bidder should insert the amount of the Guarantee in words and figures denominated in Maldivian Rufiyaa. This figure should be the same as shown in Clause 16.1 of the Instructions to Bidders.

we undertake to pay to the Purchaser up to the above amount upon receipt of his first written demand, without the Purchaser's having to substantiate his demand, provided that in his demand the Purchaser will note that the amount claimed by him is due to him owing to the occurrence of one or any of the three conditions, specifying the occurred condition or conditions.

This Guarantee will remain in force up to and including the date ……………………. days after the deadline for submission of bids as such deadline is stated in the Instructions to Bidders or as it may be extended by the Purchaser, notice of which extension(s) to the Bank is hereby waived. Any demand in respect of this Guarantee should reach the Bank not later than the above date.

DATE…………………………… SIGNATURE OF THE BANK

WITNESS ……………………… SEAL

[signature, name, and address]

.6.7 ފަރާތުގެންނާ ގުޅިގެން ކަނޑާ ހަވާލުވާ ގޮތް

Form of Performance Bank Guarantee (Unconditional)

To: ……..
[name &address of Purchaser]
……..
……..

WHEREAS ……. *[name and address of Supplier]* (hereinafter called "the Supplier") has undertaken, in pursuance of Contract No. …… dated …… to execute …… *[name of Contract and brief description of Works]* (hereinafter called "the Contract");

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with his obligations in accordance with the Contract;

AND WHEREAS we have agreed to give the Supplier such a Bank Guarantee;

NOW THEREFORE we hereby affirm that we are the Guarantor and responsible to you, on behalf of the Supplier, up to a total of *…….. *[amount of Guarantee]* …… *[amount in words]*, such sum being payable in the types and proportions of currencies in which the Contract Price is payable, and we undertake to pay you, upon your first written demand and without cavil or argument, any sum or sums within the limits of …… *[amount of Guarantee]* as aforesaid without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

*An amount is to be inserted by the Guarantor, representing the percentage of the Contract Price specified in the Contract, in Maldivian Rufiyaa.

We hereby waive the necessity of your demanding the said debt from the Supplier before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the Contract or of the Works to be performed there under or of any of the Contract documents which may be made between you and the Supplier shall in any way release us from any liability under this Guarantee, and we hereby waive notice of any such change, addition, or modification.

This Guarantee shall be valid until the date of issue of the Defects Correction Certificate.

SIGNATURE AND SEAL OF THE GUARANTOR ……..
Name of Bank ……..
Address ……..
……..
……..
Date ……

8.6 އެއްބަސްވުމުގެ ނަމޫނާ

އެއްބަސްވުން

ނަންބަރު:

1. ތައާރަފު. 1.1. މިއީ (މަސައްކަތުގެ ތަފްސީލު) ގެތުމަށް މަސައްކަތް ހަވާލުވާ ފަރާތާއި އެކު ވެވޭ އެއްބަސްވުމެކެވެ.

2. އެއްބަސްވުމުގެ ބައިވެރިން. 2.1. މި އެއްބަސްވުމުގައި މަސައްކަތް ހަވާލުކުރި ފަރާތްކަމުގައި ބަޔާންކުރެވިފައިވަނީ، ނޭޝަނަލް ސެންޓަރ ފޯރ އިންފޮރމޭޝަން ޓެކްނޮލޮޖީއެވެ.

2.2. މަސައްކަތާއި ހަވާލުވާ ފަރާތް ކަމަށް ބަޔާންކުރެވިފައިވާނީ (ކުންފުނި ނުވަތަ ވިޔަފާރީގެ ނަން)

3. އެއްބަސްވުމުގައި ހިމެނޭ ތަކެއްޗާއި މަސައްކަތްތައް 3.1. މަސައްކަތް ހަވާލުކުރި ފަރާތުން (ތާރީޚް) ވަނަދުވަހު ކުރި އިޢުލާން (ނަންބަރު) އާއި ގުޅިގެން މަސައްކަތާއި ހަވާލުވިފަރާތުން ހުށަހަޅާފައިވާ، (މި އެއްބަސްވުމުގެ ޖަދުވަލު 1 ގައި އެއްކަރުދާސްކޮށްފައިވާ) ޕްރޮޕޯޒަލްގައިވާ ތަކެތި/މަސައްކަތް ހަވާލުކުރިފަރާތަށް ސަޕްލައިކޮށްދިނުން.

4. މަސައްކަތުގެ އަގު. 4.1. ޖަދުވަލު 1 ގައިވާ މަސައްކަތްކުރުމަށް މަސައްކަތުގެ އަގު ގޮތުގައި ކަނޑައަޅާފައިވަނީ (އަގު) އެވެ.

5. މަސައްކަތުގެ މުއްދަތު. 5.1. ޖަދުވަލު 1 ގައި ބަޔާންކޮށްފައިވާ މަސައްކަތް (މުއްދަތު) ދުވަހުގެ ތެރޭގައި (ރަސްމީ ބަންދު ދުވަސްތައް ހިމަނައިގެން) ނިންމުމަށް މަސައްކަތް ހަވާލުވި ފަރާތުން އެއްބަސްވެއެވެ.

(ހ) އެއްބަސްވުމުގައި ސޮއި ކުރާ (ތާރީޚް) އެވެ.

(ށ) އެއްބަސްވުމުގައިވާ މަސައްކަތް ނިންމަންޖެހޭ (ތާރީޚް) އެވެ.

6. މަސައްކަތަށް ފައިސާދެއްކުން 6.1. މަސައްކަތް އެއްބަސްވުމާ ފުރިހަމަކޮށް ނިންމުނުކަމަށް މަސައްކަތް ހަވާލުކުރި ފަރާތުން ނިންމުމުން، މަސައްކަތް ހަވާލުވި ފަރާތުން މަސައްކަތުގެ ބިލް އަސްލު، މަސައްކަތް ހަވާލުކުރި އޮފީހަށް ހުށަހެޅުމުން އިންވޮއިސް ނުވަތަ ރިސެޕްޝަން ހުށަހަޅަންވާނެއެވެ. އަދި މި ބިލަށްވާ ފައިސާ 30 (ތިރީސް) ދުވަހުގެ ތެރޭގައި ދައްކައި ނިންމަންވާނެއެވެ.

7.	ތިލަދުންފުށި ގ.ރ.	7.1. ކުރިން ދަނޑުވެ ދާ ގޮތަށް ދަނޑުގެ ބައިތަކުގެ ތެރެއިން ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި
		7.2. ކަނޑާ ދުރުގައި ހުންނަ ދަނޑުތަކުގެ ބައިތަކުގެ ތެރެއިން ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި
8.	ދަނޑުގެ ބައިތަކުގެ ތަފްޞީލް.	8.1. ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައިތަކުގެ ތެރެއިން ހުދުވެ (ދަނޑު، ހުދުބަދަ ނުވަތަ ދަނޑަކާ) ގުޅިގެން ދިއުމަށް ދަނޑުގެ ތެރެއަށް ވަދެ ދަނޑުގެ ތެރެއިން ދަނޑުގެ ބައި ކަނޑާ ދުރުގައި ހުންނަ ދަނޑުގެ ބައިތަކަށް ދާ ގޮތަށް ހުދުބަދަ ބަނދަރު ގުޅުވައި ދެ ދަނޑުގެ ބައިތަކުގެ ތެރެއިން ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި

(ހ) ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައިތަކުގެ ތެރެއިން ދަނޑުގެ ބައިތަކުގެ ތެރެއަށް ދާ ގޮތަށް ހުދުބަދަ ބަނދަރު ގުޅުވައި ދަނޑުގެ ބައި ދަނޑުގެ ބައިތަކަށް ވެސްވާ ވިހާރުގެ ފުށުގައި ހުންނަ ދަނޑުގެ ބައި

(ށ) ވެސްވާ ކަނޑާ ދުރުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި

(ނ) ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައިތަކުގެ ތެރެއިން ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި

(ރ) ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައިތަކުގެ ތެރެއިން ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި

(ބ) ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައިތަކުގެ ތެރެއިން ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި

(ဘ) ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައިތަކުގެ ތެރެއިން ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި ދ. ހުދުވެ ދ. ދިގުލަ ކ. 1 ގެ ދަށުގައި ހުންނަ ދަނޑުގެ ބައި

8.2. ލިޔުމުން ހުށަހަ ބަޔާން ހުށަހަޅާ ކޮންޓްރެކްޓަށް ބަދަލެއްގެ ގޮތުގައި ތަކެއްޗާ ގުޅިގެން ކުރިއަށް ގެންދާ ކަންކަމުގެ ފައިސާ *10.55* ގައި ބަދަލުކުރެވޭނެ ހަމަނައިސް.

8.3. ލި ތާރީޚުގެ ދެ ބަދަލުގެ ބަޔާން.

9. ކަނޑައެޅިފައިވާ ގަދަ ވާހަކަ ދެއްކުމުގެ ސިފައިން.

9.1. ލިޔުމުން ހަމަވާކަށް ހަވާލުކުރާ ތަކެއްޗާ ގުޅިގެން ކުރިއަށް ގެންދާ ކަންކަމުގައި ކަނޑައެޅިފައިވާ ގަދަ ވާހަކަ ދެއްކުމުގެ ސިފަ ބަދަލުކުރެވޭނެ ހަމަނައިސް.

9.2. ހަފްތާ ތެދުވެ ކަނޑައެޅިފައިވާ ގަދަ ވާހަކަ ދެއްކުމުގެ ސިފައިގައި ހަމަ *10.71* ވަނަ ދުވަހު ކަމުގައި ވާ ގޮތަށް ލިޔުމުން ބަދަލުކުރެވޭނެ ހަމަނައިސް ތަކެއްޗާ ގުޅިގެން ކުރިއަށް ގެންދާ ކަންކަމުގެ ފައިސާ ދައްކަންވާ ގޮތް.

9.3. ދުވަހަކަށް *5،000،000/-* ދުވަހުގެ ދަށުން ކަނޑައެޅިފައިވާ ތަކެއްޗާ ގުޅިގެން ކަނޑައެޅިފައިވާ ގަދަ ވާހަކަ ދެއްކުމުގެ ދުވަހަކަށް 0.005 (ފަސްދިހަ ހާސް ތިންސަތޭ) ގ ގުޅަންވާ ދުވަސް ގާތަށް ކަނޑައެޅިފައިވާ ގަދަ ވާހަކަ ދެއްކުމުގެ ދުވަހަކަށް ދައްކަންވާ ގޮތް ކަނޑައެޅުން.

ލިޔުމުން ބެލެހެއްޓުމުގެ ދަށުން = CP*0.005*LD

ތަނާ ދުވަހަކަށް *5،000،000/-* ދުވަހުގެ ދަށުން ކަނޑައެޅިފައިވާ ގަދަ ވާހަކަ ދެއްކުމުގެ ދަށުން ފަސްދިހަ ހާސް ތިންސަތޭ (ފަސްދިހަ ހާސް ތިންސަތޭ) ގ ގުޅަންވާ ދުވަސް ގާތަށް ކަނޑައެޅިފައިވާ ގަދަ ވާހަކަ ދެއްކުމުގެ ދުވަހަކަށް ދައްކަންވާ ގޮތް ކަނޑައެޅުން.

ލިޔުމުން ބެލެހެއްޓުމުގެ ދަށުން = CP*0.0025*LD

CP (ކޮންޓްރެކްޓް ވެލިއު): ކޮންޓްރެކްޓުގެ ދުވަހަކަށް

LD (ލީޑް ޓައިމްސް): ކޮންޓްރެކްޓުގެ ދުވަހަކުން ލިޔުމުން ހަވާލުކުރާ ކަންކަމުގެ

9.4. • ލި ދުވަސް ލި ބަދަލުގެ ދަށުން ކަނޑައެޅިފައިވާ ގަދަ ވާހަކަ ދެއްކުމުގެ ދުވަހަކަށް ލިޔުމުން ބެލެހެއްޓުމުގެ ދަށުން ދައްކަންވާ ގޮތް (ފައިނަލް ކަނޑައެޅުން) ކޮންޓްރެކްޓުގެ ދަށުން ދައްކަންވާ ގޮތް ކަނޑައެޅުން.

9.5. ދަށުން ދައްކަންވާ ދުވަސް ގާތަށް ދަށުން ދައްކަންވާ ގޮތަށް ކަނޑައެޅިފައިވާ ގަދަ ވާހަކަ ދެއްކުމުގެ ދަށުން *15%* (ފަސްދިހަ ސަތޭކަ) ކަނޑައެޅި ބަދަލެއް ދައްކަންވާ ގޮތް.

9.6. ބަދަލުކުރެވޭ ދުވަހަކަށް ކޮންޓްރެކްޓުގެ ދަށުން *15%* (ފަސްދިހަ ސަތޭކަ) ކަނޑައެޅި ލިޔުމުން ބެލެހެއްޓުމުގެ ދަށުން ދައްކަންވާ ގޮތް، ކޮންޓްރެކްޓުގެ ދުވަހަކުން

ކޮންޓްރެކްޓަރުގެ އަތުން ވަކިކުރެވިދާނެއެވެ. އަދި ކޮންޓްރެކްޓަރ ހިލާފުވި ފަރާތުގެ ޒިންމާދާރުވުމަށް ޕަރފޯމަންސް ސެކިއުރިޓީ ނުވަތަ އެހެން ސެކިއުރިޓީއެއް ވާނަމަ ދޫކުރުން ހިފެހެއްޓޭނެއެވެ. މީގެ ތެރޭގައި ކޮންޓްރެކްޓަރ ދައްކަންޖެހޭ ލިކުއިޑޭޓެޑް ޑެމޭޖަސް ނުހިމެނޭނެއެވެ.

9.7. މި އެއްބަސްވުމުގައިވާ ކަންކަން ހާސިލްވަންދެން ނުވަތަ އެއްބަސްވުން ނިމުމަކަށް ގެންނަން ދެން މި އެއްބަސްވުން ދެމި އޮންނާނެއެވެ.

10. އެއްބަސްވުމުގެ މުއްދަތު

10.1. މިއެއްބަސްވުމުގެ މުއްދަތުގައި މިއެއްބަސްވުމުގެ ސަބަބުން ނުވަތަ މިއެއްބަސްވުމާއި ގުޅިގެން ނުވަތަ މިއެއްބަސްވުމުގައި ބަޔާންކޮށްފައިވާ ކަންތައްތައް ހައްލުކުރާނީ ދެފަރާތުގެ ސުލްހަވެރިކަމާއެކު ވާހަކަ ދައްކައިގެންނެވެ. އެފަދައިން ވާހަކަދެއްކުމުގައި އަދި ގޮތެއް ނިންމުމުގައި ދެފަރާތުންގެ އައްޔަންކުރާ ފަރާތެއް ނުވަތަ ފަރާތްތަކެއް ބައިވެރިކުރެވިދާނެއެވެ.

11. ދިމާވާ މައްސަލަ ހައްލުކުރާނެ ގޮތް

11.1. ސުލްހަވެރި ނިމުމެއް މައްސަލައަކަށް ނުހޯދިއްޖެނަމަ، ދިވެހިރާއްޖޭގެ ކަމާބެހޭ ކޯޓަށް މައްސަލަ ހުށަހަޅައި ޝަރުޢީ ނިޒާމުގެތެރެއިން މައްސަލަ ނިންމުމަކަށް މި އެއްބަސްވުން ހުށަހަޅާ ނިމޭއެވެ.

12. މުޢާމަލާތްކުރުން.

12.1. މި އެއްބަސްވުމުގައި ޝާމިލުވާ ފަރާތްތަކުން މިއެއްބަސްވުމާއި ގުޅިގެން އެއް ފަރާތުން އަނެއް ފަރާތަށް އަންގަންޖެހޭ އެންގުންތައް އާއްމުގޮތެއްގައި އަންގާނީ ލިޔުމުންނެވެ.

މަތީގައިވާ އެއްގޮތަށް ކަންތައްތަކުގެ މައްޗަށް އެއްބަސްވެ މި އެއްބަސްވުމުގައި (ތާރީޚް) ގެ (ދުވަސް) ދުވަހު ދެފަރާތުން ސޮއިކުރީމެވެ.

މަސައްކަތް ހަވާލުކުރި ފަރާތް	މަސައްކަތާއި ހަވާލުވި ފަރާތް
(މަސައްކަތް ހަވާލުކުރި ފަރާތުގެ ނަން)	(މަސައްކަތާ ހަވާލުވި ފަރާތުގެ ނަން)
ނަން :	ނަން :
މަޤާމް :	މަޤާމް :
ހެކިން:	މަސައްކަތާއި ހަވާލުވި ފަރާތް

ދަނޑުވަށުގެ ހުރިހާ ތަފާތުތަކާ	ދަނޑުވަށުގެ ތެރެ
ހާލަ:	ހާލަ:
ތަރިން:	ތަރިން :
ތަރިއަށް ދޭ ގޮތް :	ތަރިއަށް ދޭ ގޮތް :