ﺇﻧﺪﻳﺮﺍ ﮔﺎﻧﺪﻱ ﻣﻴﻤﻮﺭﻳﻞ ﻫﺴﭙﺘﺎﻝ

INDIRA GANDHI MEMORIAL HOSPITAL

Kan’baa Aisaarani Hingun, Male’, Republic of Maldives

ތަކެތި Endpoint Security System ގަނެވުނު ކުންފުނިން ހިފަހައްޓާ ސާވިސް ހިންގުމާ ގުޅޭ

137-IU/PR/2020/09 ދާއިރާ ނަންބަރ

137/PR/2021/G-06: ގުޅުމުގެ ނަންބަރ

ސެކްޝަން 1

1.4 ތިރީގައި ބަޔާންކޮށްފައިވާ ސްޕެސިފިކޭޝަނަށް Endpoint Security System ހޯދަން ބޭނުންވެއެވެ.

Endpoint Security System

	Count	License Type
VDI's	500 Vm	Hybrid Cloud Security, Desktops
Physical desktops	50 Desktops	Endpoint Security Business Advanced
Hyper V	25 Servers	Endpoint Security Business Advanced
AHV	15 Nutanix Hyper V	Nutanix Hyper V

Note: This software is with one year license subscription and annual Renewal is required

General requirements:

1 Agentless anti- malware software for virtual environments

2 Agent-based anti- malware software for virtual environments

3 Centralized management, monitoring and updating of software

4 Ability to update anti-malware databases and network attack patterns

5 Administrator and User documentation in English

6 Software Defined Networking compatibility

7 Solution required to be in accordance with the requirements of the General Data Protection Regulation (GDPR) for the protection of virtual infrastructures.

8 Solution must have a protection for private cloud and public cloud which includes AWS and MS Azure.

9 Solution must have a single management console for the protection management on private and public cloud which includes AWS and MS Azure

Light Agent Anti-Malware solution

2 Requirements software for virtual environments:
- Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-bit)
- Windows 10 Pro / Enterprise / Enterprise LTSB / RS1 / RS2 / RS3 / RS4 (32 / 64-bit)
- Windows Server 2012, all revisions (in full mode) (64-bit)
- Windows Server 2012 R2, all revisions (in full mode) (64-bit)
- Windows Server 2016, all revisions (in full mode) (64-bit)
- Debian GNU / Linux 8.9 (32 / 64-bit)
- Debian GNU / Linux 9.1 (64-bit)
- Ubuntu Server 16.04 LTS (32 / 64-bit)
- Ubuntu Server 18.04 LTS (64-bit)
- CentOS 6.9 (64-bit)
- CentOS 7.4 (64-bit)
- Red Hat Enterprise Linux Server 7.4 (64-bit)
- SUSE Linux Enterprise Server 12 Service Pack 1 (64-bit)

3 Resident anti-malware monitoring.

4	Protection against rootkits and auto dialers to paid sites.
5	Suggested solution for Linux and Microsoft Windows must have File Integrity Monitor that can guarantee the integrity of system files, logs and critical applications by tracking unauthorized changes in important files and directories
6	Heuristic analyzer to detect and block previously unknown malware.
7	Transfer of anti-malware scanning and other resource-intensive tasks from all guest virtual machines to a separate machine.
8	Automatic detection and connection to a functioning protection machine, including one operating on a different host if the main protection machine is unavailable.
9	Ensuring continuity of file protection during short-term unavailability of the protection machine by logging all file operations on the protected virtual machine during the period of unavailability, and automatic scanning of all changes after access is restored.
10	Cloud-based protection against new threats, allowing the application to access a developer's special resources in order to obtain file verdicts during real-time or scheduled scanning.
11	Protection of e-correspondence from malware by checking incoming and outgoing traffic on IMAP, SMTP, POP3, MAPI, NNTP protocols regardless of the email client.
12	Protection of web traffic: scanning of objects - including the use of heuristic analysis - sent to the user's computer via HTTP and FTP protocols, with the ability to configure trusted sites.
13	Blocking banners and pop-ups on web pages.
14	Detection and blocking of phishing sites.
15	Protection against yet unknown malicious programs based on their behavior.
16	Ability to determine anomalous behavior by an application by analyzing its execution sequence. Ability to roll back malware operations during treatment.
17	Ability to restrict the privileges of executable programs such as writing to the registry or accessing files and folders. Automatic detection of restriction levels based on the reputation of the program.
18	Built-in firewall that allows network packet rules to be set for specific protocols (TCP, UDP) and ports. Creation of network rules for specific programs.
19	Protection against hacker attacks by using a firewall with an intrusion detection and intrusion prevention system (IDS/IPS) and network activity rules for the most popular applications when working on any type of computer networks, including wireless networks.
20	Component enabling the creation of special rules to block the installation and/or running of a program. The component should be able to control the application via program path, metadata, MD5 checksum, and predefined categories of applications provided by the vendor. It should also allow exceptions to the rules for specific AD users.
21	Monitoring user activity with external I/O devices by the type of device and/or the bus used including the ability to create a list of trusted devices by their ID and the ability to grant privileges to use external devices to specific AD users.
22	Monitoring user activity on the Internet including blocking or permitting access to certain resources as well as the ability to block certain types of information (audio, video, etc.). The software should allow the implementation of time intervals for control, and the ability to assign them only to specific AD users.
23	Centralized updates allowing part of an anti-malware database to be stored on a protection machine.
24	Running a special task to detect vulnerabilities in the applications installed on a computer with the option of submitting a report on any vulnerabilities found.
25	Integration with Windows Update to patch detected vulnerabilities.
26	The ability to remotely install and distribute anti-malware software components on all protected virtual machines without using third-party tools.
27	On-schedule scanning of all virtual machines.
28	Availability of information about scanned files on the protection machine to prevent re-scanning of the same files on different virtual machines.
29	Blocking, neutralization and removal of malware, notification of administrators.
30	A single management console for all protection components.

31	A single centralized management console for both virtual environments and physical workstations.
32	Detailed information about events on virtual machines and protection tasks execution.
33	Ability to apply different security settings for different groups of virtual machines.
34	Storage of backup copies of deleted files.
35	Support for VMware technology: vMotion, Distributed Resource Scheduler
36	Support for Citrix technology: Virtual User Drive, Citrix Receiver, Multi-stream ICA, XenMotion Live Migration, Automated VM protection and recovery, Dynamic memory control.
37	Support for Hyper-V technology: Live migration, Cluster shared volumes, Dynamic memory, Live backup.
38	Support for rollback of antivirus databases.
39	Support for a licensing scheme according to the number of protected virtual machines and according to the number of hardware CPU cores.
40	Ability to protect virtual machines running Windows and Linux operating systems.
41	Unified administration console for efficient deployment and management of the entire IT security infrastructure.
42	Automatic Exploit Prevention that can blocks the exploitation of application vulnerabilities commonly used by cyber-criminals, dramatically increasing the overall level of protection.
43	Application startup control component that have application categorization and dynamic whitelisting, which can block apps not only by Name or by Directory path, but using advanced rules.
44	Application control must be available for both Microsoft windows desktops and Windows servers.
45	Application control for windows servers must have default whitelist logic.
46	Solution must include integrity monitoring component.
47	Default Deny support to prevent any application starting except those allowed.
48	Features that monitors the behavior of running applications and regulates their activities.
49	Built-in Extended network protection, which detects and blocks direct network attacks.
50	Built-in Extended web protection, which detects and blocks malicious URLs.
51	Suggest solution must include support for Docker
52	Checks all files during anti-malware scan (even files larger than 30 Mb).
53	Send notification by starting/launching the specified executable file.
54	Redundancy techniques, which allow reconnecting to any SVA within the infrastructure without any manual (re)configuration.
55	Sending notifications via SMS supported
56	One security policy to manage all protection modules.
57	Built-in Deferred scan queue techniques, which helps achieving 24/7/365 anti-malware protection operation.

ސެކްޝަން 2:

2.1 ބީލަމުގައި ބައިވެރިވުމަށް ފުރުޞަތު ދިނުން/ ކުރިމަތި ލުން

މި ބީލަމުގައި ބައިވެރިވާ ފަރާތަކީ އެ ޚިދުމަތެއް ފޯރުކޮށްދިނުމަށް ހުއްދަ ލިބިފައިވާ، ދާއިމީގޮތުގައި ހިނގަމުންދާ ތަޖުރިބާކާރުކަމުގައިވާންވާނެއެވެ. އަދި ސަރުކާރުގެ ގަވާއިދާއި އެއްގޮތްވާގޮތުގެމަތިން، ސަރުކާރުގެ ތަންތަނުން މަސައްކަތްތަކުން ދިނުމަށް އެއްބަސްވާ ފަރާތެއްކަމުގައިވާންވާނެއެވެ.

2.2 ބީލަން ހުށަހަޅާނެގޮތް

މިބީލަން ކުރިއަށް ގެންދެވޭނީ 02 "ބައިގަ" އުސޫލުންނެވެ. އެއީ ޕްރީކޮލިފިކޭޝަން/ޓެކްނިކަލް އިވެލުއޭޝަނަށް ފަހު ޕްރައިސް ބިޑް އިވެލުއޭޓްކުރުމެވެ. ބީލަން ހުށަހަޅުއްވާއިރު ޕްރީ ކޮލިފިކޭޝަން/ ޓެކްނިކަލް ކޮލިފިކޭޝަން ގައި ހިމަނަންޖެހޭ ބިޑް ޑޮކިއުމަންޓްސްތައް (މިކަރުދާހުގެ ސެކްޝަން 05ގައި) ބަޔާންކުރާ ޑޮކިއުމަންޓްތައް ހުށަހަޅަންވާނީ ވަކި ސިޓީއުރައެއްގައެވެ. އަދި މަސައްކަތުގެ އަގު ނުލައި ކޯޓޭޝަން ހުށަހަޅަންވާނީ ވަކި ސިޓީއުރައެއްގައި، ދެ ސިޓީއުރައިގެ ބޭރުގައި ހުށަހަޅާ ފަރާތުގެ ނަމާއި، އައި.ޖީ.އެމް.އެޗް ޓެންޑަރ ނަންބަރާ Endpoint Security System ލައިސަންސް ހޯދުމާއި ރިނިއުކުރުން ގުޅޭ ބިޑް ކަމާއި އަދި އިޢުލާން ނަންބަރު ޖަހާފައި އޮންނަންވާނެއެވެ. މިދެންނެވި ގޮތަށް ހުށަހަޅާފައިވާ ހުރިހާ ފަރާތްތަކުގެ ބިޑް ބަލައިގަނެ ޕްރީކޮލިފިކޭޝަން/ޓެކްނިކަލް ކޮލިފިކޭޝަން ގައި ބައިވެރިކުރެވޭނެއެވެ. އަދި 2.3ވަނަ މާއްދާގައި، ޕްރީކޮލިފިކޭޝަން/ޓެކްނިކަލް ކޮލިފިކޭޝަންގައި ބަޔާންކުރާގޮތަށް ކްރައިޓީރިއާއިން ފާސްވާ ފަރާތްތަކަށް ޕްރައިސް ބިޑް އިވެލުއޭޝަންގައި ބައިވެރި ކުރެވޭނެއެވެ.

ނޯޓް: ޕްރޮޕޯސަލް ހުށަހަޅާއިރު މައުލޫމާތު ކަރުދާހުގައި ހިމެނިފައިވާ ބިޑް ހުށަހަޅާފޯމް ފުރިހަމަކޮށްގެން ހުށަހަޅަންވާނެއެވެ.

2.3 ޕްރީކޮލިފިކޭޝަން/ޓެކްނިކަލް ކޮލިފިކޭޝަން ކުރިއަށް ގެންދާނެ ގޮތް

މިބައިން މާކްސް ކަނޑައެޅިފައި ނުވާނެއެވެ. އެހެން ނަމަވެސް ޕްރީ އަދި ޓެކްނިކަލް ކޮލިފިކޭޝަންގައި ހުށަހަޅަންޖެހޭ ލިޔެކިޔުންތައް ހަމައަށް ހުރުން ލާޒިމުވާނެއެވެ. މިގޮތުން ހުރިހާ ޑޮކިއުމަންޓްސް ނުވަތަ ސެކްޝަން 05 ގައި ބަޔާންކުރާ އެންމެހައި ކަންކަން ފުރިހަމަކޮށްފައިވާ ބިޑްތައް އިވެލުއޭޝަން ޓީމުން ބަލައި ކްރައިޓީރިއާއިން ފާސްވާ ފަރާތްތަކުގެ ޕްރައިސް ބިޑް އިވެލުއޭޝަންގައި ބައިވެރިކުރެވޭނެއެވެ.

2.4 ޕްރައިސް ބިޑް އިވެލުއޭޝަން ކުރިއަށް ގެންދާނެގޮތް

އަގަށް މާކްސްދޭނީ އެންމެ ކުޑައަގެއް ހުށަހަޅާފަރާތަކަށް ދިނުމުގެ ޕްރޮރާޓާ އުސޫލުންނެވެ. ޕްރައިސް ބިޑްތައް އިވެލުއޭޓްކުރެވޭނީ ޕްރީކޮލިފިކޭޝަން/ ޓެކްނިކަލް ކޮލިފިކޭޝަނުން ފާސްވެފައިވާ ފަރާތްތަކުގެ ބިޑްތަކެވެ. މިގޮތުން ސެކްޝަން 06 ގައި ބަޔާންކުރާ މާކްސް ޕްރޮރާޓާ އުސޫލުން ދެވޭނެއެވެ.

2.5 ބީލަން ހުށަހެޅުމުގެ ގަޑިއާއި ތަން

މިބީލަން ކުރިމަތިލާ ފަރާތްތަކުން ސެކްޝަން 03 ގައި ބަޔާންކޮށްފައިވާ ގަޑިތަކަށް ސަބްމިޓްކުރަން ޖެހޭނެއެވެ. އަދި ބިޑް ހުށަހަޅަން ކަނޑައެޅިފައިވާ ވަގުތުގެ ކުރިން ބިޑްހުށަހަޅަންކަނޑައެޅިފައިވާ ތަނަށް ހާޒިރުވާންވާނެއެވެ. ބިޑްތައް ހުޅުވާނީ ހުރިހާ ފަރާތްތަކެއްގެ ހާޒިރުގައެވެ. އަދި ވަގުތު ހަމަވުމުން ހާޒިރުވާ ފަރާތްތަކުގެ ބިޑް ބަލައި ނުގަނެވޭނެއެވެ.

ސެކްޝަން 3:

ބީލަން ކުރިއަށް ދާނެ ގޮތުގެ ޓައިމްލައިން، އެކިކަންކަމަށް ކަނޑައެޅިފައިވާ ވަގުތުތައް

އިއުލާން އާންމުކުރުން	25 ފެބްރުއަރީ 2021
ސުވާލުތައް އީ-މެއިލް މެދުވެރިކޮށް ފޮނުވުން	03 މާރިޗު 2021 (14:00 ސާޢަތުމިންޖު) ގެ ނިޔަލަށް tenders@igmh.gov.mv އީމެއިލްއަށް ސުވާލުތައް ފޮނުވުން
ސުވާލުތަކަށް ޖަވާބު ފޮނުވައިދޭނެ އެންމެފަހުގެ ކުރެން	03 މާރިޗު 2021 0:00 އަށް
ބިޑު ހުށަހެޅުން/ޕްރޮޕޯސަލް ބަލައިގަތުން	04 މާރިޗު 2021 11:00ގައި ޕްރޮކިއުމަންޓް ޑިޕާޓްމަންޓްގެ މީޓިންގ ރޫމްގައި

ބިޑް ހުށަހަޅުއްވަން ގެނައުން ހާޒިރުކުރާ ފަރާތްތަކަށް ބިޑް ހުށަހެޅުމުގެ ފުރުސަތު ދެވޭނީ ނޫނަސް ވާހަކަ ދަންނަވަމެވެ.

ސެކްޝަން 4: ސިޓީއުގައި 1ގައި ހުށަހަޅަންޖެހޭ ތަކެތީގެ މަޢުލޫމާތު

4.1 ކަންފުނީގެ ޕްރޮފައިލް

4.2 މާލިއްޔަތު މިމަސައްކަތް ކުރެވޭނެ ފެންވަރުގެ ފަރާތެއްކަން އަންގައިދޭ ލިޔުމެއް ހުށަހެޅުން

4.3 މަސައްކަތުގެ ތަޖުރިބާ ހުރިމިންވަރު ދެނެގަތުމަށް ލިޔުން ހުށަހެޅުން

4.4 ކަންފުނީގެ ރަޖިސްޓްރީ ކޮޕީ

4.5 ޖީ.އެސް.ޓީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓްގެ ކޮޕީ (ޖީއެސްޓީއަށް ރަޖިސްޓަރީ ކޮށްފައިވާނަމަ)

- ސިޓީއުގައި 1ގައި ހުށަހަޅަންޖެހޭ އެއްވެސް ޑޮކިއުމަންޓެއް މަދުނަމަ އެ ބިޑު ޑިސްކޮލިފައިވާނެއެވެ. އަދި ޕްރައިޒް ބިޑު އިވެލުއޭޓް ނުކުރާނެއެވެ.
- އަގު ހުށަހަޅާފައި އޮންނަންވާނީ ސިޓީއުގައި 2 ގައެވެ.

ސެކްޝަން 5: ޕްރީ ކޮލިފިކޭޝަން/ ޓެކްނިކަލް ބިޑުގައި ހުށަހަޅާ ޑޮކިއުމަންޓްތަކުގެ ތަފްސީލު.

5.1 ކަންފުނީގެ ޕްރޮފައިލް

5.1.1 ކަންފުނީގެ ނަމާއި ފުރިހަމަ އެޑްރެސް، ފޯން ، ފެކްސް އަދި އީމެއިލް އެޑްރެސް ބަޔާންކުރުން

5.1.2 ކަންފުނީގެ ވެރިޔަކު އިން ފެށިގެން މަތީގެ ފަރާތްތަކުގެ ނަމާއި ކަންފުނީގެ މަޤާމު، އައި.ޑީ ކާޑު އަދި ފޯނުނަމްބަރު.

5.1.3 ކަންފުނީގެ މައިގަނޑު މަސައްކަތްތައް

5.1.4 ކަންފުނީގެ ރަޖިސްޓްރީ ނަމްބަރު އަދި ކަންފުނި އުފެދުނު ތާރީޚް

5.1.5 ޓެކްސް ކްލިއަރަންސް ލިޔުން ނުވަތަ ޓެކްސް ދައްކާފައިވާކަމުގެ ރިސީޓްތައް

5.1.6 <u>އޮތޯރައިޒް ޑިސްޓްރިބިއުޓަރ ލެޓަރ</u>

މިގެ އިތުރުން ބިޑުގައި ހުށަހަޅަންބޭނުންވާ އިތުރު މައުލޫމާތު *

- ކަންފުނީގެ ޕްރޮފައިލްގައި ބޭނުންވާ މައުލޫމާތު ފުރިހަމަކޮށްދީފައި އިސްކަންދެއްވާނެއެވެ.

5.2 މާލިއްޔަތު މިމަސައްކަތް ކުރެވޭނެ ފެންވަރުގެ ފަރާތެއްކަން އަންގައިދޭ ލިޔުމެއް ހުށަހެޅުން

5.2.1 ޕްރޮޖެކްޓްކޮށްދޭން ހުށަހަޅާފައިވާ އަގުގެ 30% ބޭނުން އެކައުންޓްގައި ހުރިކަން އަންގައިދޭ ލިޔުމެއް (ބޭނުން ސްޓޭޓްމަންޓް ނުވަތަ ބޭންކުގެ ލިޔުމެއް) * ބިޑް ހުށަހަޅާއިރު މިކަމުދާހުގައިވާ ފޯމެޓް ފުރިހަމަކުރަންވާނެއެވެ

5.3 މަސައްކަތުގެ ތަޖުރިބާ ހުރިމިންވަރު ދެނެގަތުން

ވޭތުވެދިޔަ 3 އަހަރު ދުވަހުގެ ތެރޭގައި، މަސައްކަތާއި ގުޅުންހުރި ގޮތުން (އައި.ޖީ ސްކޫލްތަކަށް ފަރު ޑެލިވަރުކުރުން) މަސައްކަތްތަކުގެ އަގު 10،000.00ރ (ދިހަހާސް) ރުފިޔާ އަށްވުރެ ދަށްނޫން މަސައްކަތްތަކެއް ނިންމާފައިވާކަމުގެ މަދުވެގެން 3 ލިޔުން ހުށަހެޅުން (އެމަސައްކަތެއްކުރުމުގެ ފަރާތުން ދީފައިވާ ލިޔުންތަކެއް)ހުށަހެޅުން.

- މިބައިން 03 ލިޔުން ހަމަނުވާ ކަމުގައިވާނަމަ ޕޮއިންޓް ނުދެވޭނެއެވެ. އަދި މަސައްކަތް ކުރުމަށް ފަރާތުން ދީފައިވާ ލިޔުންތަކުގައި މަސައްކަތް ނިންމިކަން އެނގެން ނެތްނަމަވެސް އަމަލުކުރެވޭނީ މިފަދައިންނެވެ.

ސެކްޝަން 6:

ޕްރައިސް ބިޑް އަދި ކޮލިފައިވުން

ޕްރައިސް އިވެލުއޭޝަންގައި ބައިވެރި ކުރެވޭނީ މަތީގައި ބަޔާންކޮށްފައިވާ ޕްރީކޮލިފިކޭޝަން/ޓެކްނިކަލް ކޮލިފިކޭޝަން އިން ފާސްވާ ބިޑްތަކެވެ.

ސެކްޝަން 7: ބިޑް އިވެލުއޭޝަން

މިމަސައްކަތް ހަވާލުކުރާނީ ފަރާތެއް ހޮވުމަށް ހަމަޖެހިފައިވާ ތިރީގައި މިވާ އުސޫލުން ބިޑް ޕްރޮޕޯސަލް ދިރާސާކުރުމަށްފަހު އެންމެ އެކަށީގެންވާ ފަރާތެއްކަމަށް ނިންމާ ފަރާތަކަށެވެ.

7.1 ޕްރީކޮލިފިކޭޝަން ކްރައިޓީރިއާ އިން ފާސްވުން

7.1.1 މާލީ ގޮތުން މިމަސައްކަތުގައި ފަރާތެއްކަން ދެނެގަތުމަށް ހުށަހަޅާފައިވާ ލިޔުންތަކުން

- ޕްރޮޖެކްޓްކޮށްދޭން ހުށަހަޅާފައިވާ އަގުގެ 30% ބޭނުން އެކައުންޓްގައި ހުރިކަން އަންގައިދޭ ލިޔުމެއް (ބޭނުން ސްޓޭޓްމަންޓް ނުވަތަ ބޭންކުގެ ލިޔުމެއް)

7.1 ވޭތުވެދިޔަ 3 އަހަރު ދުވަހުގެ ތެރޭގައި، މަސައްކަތާއި ގުޅުންހުރި ގޮތުން (އައި.ޖީ ސްކޫލްތަކަށްފަރު) މަސައްކަތްތަކުގެ އަގު 10،000.00ރ (ދިހަހާސް) ރުފިޔާ އަށްވުރެ ދަށްނޫން މަސައްކަތްތަކެއް ނިންމާފައިވާކަމުގެ މަދުވެގެން 3 ލިޔުން ހުށަހެޅުން (އެމަސައްކަތެއްކުރުމުގެ ފަރާތުން ދީފައިވާ ލިޔުންތަކެއް)ހުށަހެޅުން.

އަގު އިވެލުއޭޝަން ކުރުމުގައި ބައިވެރި ކުރެވޭނީ މަތީގައި ބަޔާންކޮށްފައިވާ ޕްރީކޮލިފިކޭޝަނުން ފާސްވާ ބިޑްތަކެވެ.

އިވެލުއޭޝަން ކުރެވޭނީ އެންމެ ކުޑައަގެއް އަދި ކުރު މުއްދަތެއް ހުށަހަޅާފައިވާ ފަރާތަކަށް ޖީއެސްޓީ ހިމަނައިގެން ޕްރޮޖެކްޓް އުސޫލުންނެވެ.

1	އަގު	95 ޕޮއިންޓް
	ޑެލިވަރީ	05 ޕޮއިންޓް

ސެކްޝަން 8:

ބިޑަން ބާޠިލު ކުރެވިދާނެ ކަންތައްތައް

8.1 ހުށަހަޅާފައިވާ މައުލޫމާތުތަކުގައި ޙަޤީޤަތާއި ޚިލާފު މައުލޫމާތުތައް ވުން.

8.2 ޚިދުމަތްދޭފަރާތާއި، ތިމާގެކަމުގެ ނުވަތަ ވިޔަފާރީގެ އެއްވެސް ގުޅުމެއް، މިތަނުގެ ވެރިޔަކާއި ހުރި އެކަމުގެ ސާފު މައުލޫމާތު ދިނުމުން ހުށަހަޅާފައިނުވުން.

8.3 ބޭނުންވާ ރިކުއަރމަންޓް/ކްރައިޓީރިއާ ފުރިނުވާ އަދި ބޭނުންވާ ސްޕެސިފިކޭޝަން ފުރިހަމަނުވާ ބިޑުތައް

ސެކްޝަން 9:

ބިޑް އެވޯޑް ކުރުން

9.1 ބިޑް އިވެލުއޭޝަންކުރުމުން، ބިޑް ކޮމިޓީގެ ފާހަގައާއި، ބިޑް ކޮމިޓީގެ ނަމާ ފާހަގަކޮށްފައިވާ ފަރާތަށް އެކަން އަންގާނެއެވެ.

9.2 ބިޑް އެވޯޑްކުރަން ބަލާނީ އެޕްރޫވަލްގައި ސޮއިކުރުމުންނެވެ. ބިޑް ކޮމިޓީން ރިކަމަންޑްކުރިޔަސް އެޕްރޫވަލްގައި ސޮއިކުރުމުގެ ކުރިން ބިޑް ކެންސަލް ކުރުމުގެ އިޚްތިޔާރު މި ހޮސްޕިޓަލަށް ލިބިގެންވެއެވެ.

9.3 މަސައްކަތް އެވޯޑްކުރަން ބިޑް ކޮމިޓީން ނިންމައި އެކަން ކޮންޓްރެކްޓަރަށް އަންގައިފިނަމަ އެކަން ކުރެވޭނެ ނުވަތަ އެގްރީމަންޓްގައި ސޮއިކުރަން ނައިސް ނުވަތަ މަސައްކަތުން ބައިވެ ނިންމާފައި މަސައްކަތް ދޫކޮށްލުން ނުވަތަ މަސައްކަތް ނިމުމަށް ފަސްވާ އެގްރީމަންޓް ބާޠިލުކުރެވޭފަދަ ކަމެއް ކުރިމަތިވެއްޖެނަމަ، ހަމައެއާއި އެއްގޮތަށް މަސައްކަތް ދެވަނަ ފަރާތަށް ދިނުމުގެ އިޚްތިޔާރު މި ހޮސްޕިޓަލަށް ލިބިގެންވެއެވެ.

ބިޑް ހުށަހަޅާ ފޯމު

އަންދާސީ ހިސާބު ހުށަހަޅުއްވާ އިރު މިފޯމުގައިވާ މައުލޫމާތު ފުރިހަމަކުރައްވައި އަންދާސީ ހިސާބާއިއެކު ހުށަހަޅުއްވަން އެދެމެވެ.

ކޮމްޕެނީގެ ނަން: ______________________________

އިއުލާނުގެ މައުލޫމާތު	
ޕްރޮޖެކްޓްގެ ނަން	
އިއުލާން ނަންބަރު	
އިއުލާނުގެ ތާރީޚު	
އަންދާސީ ހިސާބު ހުށަހަޅާ ދުވަސް	

އަންދާސީ ހިސާބު ހުށަހަޅުއްވަން ގަޑިއަށް ހާޟިރު ނުވާ ފަރާތްތަކަށް އަންދާސީ ހިސާބު ހުށަހެޅުމުގެ ފުރުޞަތު ދެވޭން ނޯންނާނެ ވާހަކަ ދަންނަވަމެވެ.

އަންދާސީ ހިސާބާއި އެކު ހުށަހަޅުއްވަންޖެހޭ ލިޔުންތަކުގެ ޗެކްލިސްޓް

✓	ލިޔުން	ސަފުހާ ނަންބަރު
	ކޯޓޭޝަން	
	ކޮމްޕެނީ ޕްރޮފައިލް	
	ކޮމްޕެނީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓްގެ ކޮޕީ	
	ޖީ.އެސް.ޓީ ރަޖިސްޓްރޭޝަންގެ ކޮޕީ	
	މާލިއްޔަތު މިމަސައްކަތަށް ކުރުވޭނޭ ފަންނުވެރިންގެ ފަރާތްތަކުން އެންގައިދޭ ލިޔުމެއް ހުށަހެޅުން (މަޢުލޫމާތު ކަރުދާހުގައިވާ ފޯމާއި އެއްގޮތަށް)	
	މަސައްކަތުގެ ތަޖުރިބާ ހުރިމިންވަރު ދެނެގަތުމަށް ލިޔުން ހުށަހެޅުން (މަޢުލޫމާތު ކަރުދާހުގައިވާ ފޯމާއި އެއްގޮތަށް)	

މިގޮތުން މިއަންދާސީ ހިސާބުގައި ހިމަނަންޖެހޭ ޓެކްނިކަލް މަޢުލޫމާތު ގެނެސްދިނުން ބައެއް ހުށަހަޅާފައިނުވާ ނަމަވެސް މުޅިން ފުރިހަމަ ނުވާފަރާތްތަކަށް، ބިޑް އިވެލުއޭޝަން ކޮމިޓީއިން އިތުރު ބޭނުންވާ މަޢުލޫމާތު ފުރިހަމަކުރުމަށް ބައިވެރިވާ ފަރާތްތަކަށް މާކްސް ނުދެވޭނެކަމަށް ދަންނަވަމެވެ.

State YES in the submitted column against the sub-factor/requirement met

Factor	**5.2 Financial Situation**			
	Criteria			
Sub-Factor	**Requirement**	**Tenderer**	**Documentation Required**	**Submitted**
5.2.1 Financial Strength	Submission of Bank/Account Statements or bank letter proving that 30% of the proposed contract price/fund is available with the contractor	Must meet requirement	Bank/Account Statement **OR**	
			Bank Letter	

Experience – Documentation Required

Factor	5.3 Experience			
Sub-Factor	Criteria		Documentation Required	Submitted
	Requirement	Tenderer		
2.3.2 Specific Experience	Participation as contractor, management contractor, or subcontractor, in at least **3** contracts within the last **3** years, each with a value of at least **MVR10,00.00** that have been successfully and substantially completed and that are similar to the proposed Works.	Must meet requirement	Minimum 3 letters of 3 different projects within the last 3 years Awarding Body/Employer's Letter with the details of contract amount, contract duration, completion date and certification of completion	

State YES in the submitted column against the sub-factor/requirement met

Details of the letters submitted

No	Name of Contract	Awarding Body (address/ contact)	Employer (address/ contact)	Contract Figure (current MVR equivalent)	Completed date
1.					
2.					
3.					

Price Bid Format

Description	Qty	Rate	Total
		… ….	

Note:

All applicable charges +GST should be included in item rates