بسم الله الرحمن الرحيم

MALDIVES
INLAND REVENUE
AUTHORITY

މަޢުލޫމާތު ޝީޓު

1. ބީލަމާއި ބެހޭ މަޢުލޫމާތު		
1·1 އިޢުލާން	ނަންބަރު	(IUL)220-AS/1/2022/6
	އިޢުލާން ކުރި ތާރީޚް	19 ޑިސެމްބަރު 2022
1·2 އަންދާސީހިސާބު ހުށަހަޅަންޖެހޭ ތާރީޚް	ތަން	މޯލްޑިވްސް އިންލަންޑް ރެވެނިއު އޮތޯރިޓީ (މި އޮތޯރިޓީގެ ދެވަނަ ފަންގިފިލާގައި)
	އެޑްރެސް	އަމީނީމަގު، މާލެ 20379، ދިވެހިރާއްޖެ
	ތާރީޚް	31 ޑިސެމްބަރު 2022
	ވަގުތު	15:00
1·3 މަސައްކަތުގެ ތަފްސީލު		ޖަދުވަލު 3 ގައިވާ މަޢުލޫމާތާއި އެއްގޮތަށް
ތާރީޚް		19 ޑިސެމްބަރު 2022

2.	އަމަލުކުރާނެ އުސޫލު
2·1	މި އިޢުލާނުގެ ދަށުން ހޯދަން ބޭނުންވާ ތަކެތި/ޚިދުމަތުގެ ތަފްސީލު، މިކަރުދާހުގެ ޖަދުވަލު 1 ގައި ތަފްސީލުކޮށް ބަޔާންކޮށްފައިވާނެއެވެ.
2·2	ބީލަމާއި ބެހޭ އިތުރު މަޢުލޫމާތު ބޭނުންފުޅުވާނަމަ procurement@mira·gov·mv އަށް އީ-މެއިލް ކުރުމުން އެ ސުވާލުތަކުގެ ޖަވާބު އެފަރާތްތަކުގެ އީމެއިލް އެޑްރެހަށް ފޮނުވުން ފޯރުކޮށްދެވޭނެއެވެ. ފޯނު މެދުވެރިކޮށް ނަމަ 3339513 / 3020478 ގުޅުއްވުމުން އެ މަޢުލޫމާތެއް ފޯރުކޮށްދެވޭނެ.
2·3	ބީލަން ހުށަހާނީ ބީލަން ހުށަހެޅުމަށް ހަމަޖެއްސިފައިވާ ބައްދަލުވުމުގައި ބީލަން ހުށަހަޅާ ފަރާތްތަކުގެ މަންދޫބުންގެ ހާޒިރުގައެވެ.
2·4	ބީލަން ހުށަހެޅުމަށް ކަނޑައަޅާފައިވާ ސުންގަޑީގެ ކުރިން ބީލަން ހުށަހެޅުއްވުން އެދެމެވެ. ބީލަން ހުށަހެޅުމަށް ކަނޑައަޅާފައިވާ ސުންގަޑި ހަމަވުމަށްފަހު ހުށަހަޅާ ބީލަން ބަލައެއް ނުގަނެވޭނެއެވެ.
2·5	ބީލަމަށް ކުރިމަތިލާ ކޮންމެ ފަރާތަކުން ހުށަހަޅާނީ 01 (އެކެއް) ބީލަމެވެ، އެހެންނަމަވެސް އެއް ބީލަމުގައި ބޭނުން އަދަދަކަށް އޮޕްޝަން ހުށަހެޅިދާނެއެވެ. އެއްބީލަމަށްވުރެ ގިނަ ބީލަން އެއްފަރާތުން ހުށަހަޅައިފިނަމަ އެ ފަރާތަކުން ހުށަހަޅާފައިވާ ހުރިހާ ބީލަމެއް ބާތިލު ކުރެވޭނެއެވެ.
2·6	ބީލަން ހުށަހެޅުއްވާނީ ބަންދު ކޮށްފައިވާ ސިޓީއުރައެއްގައެވެ، އަދި ސިޓީއުރައިގެ ބޭރުގައި މި ދަންނަވާ މަޢުލޫމާތު ހިމަނައިފައިވާންޖެހޭނެއެވެ. ("ބީލަން ކުރާފަރާތް" "އިޢުލާން ނަންބަރު" "ބީލަމުގައި ހިމެނޭ އައިޓަމްގެ ނަން" "ބީލަން ހުށަހާ ތާރީޚް" "ބީލަން ހުށަހާ ގަޑި") މިހެން ބޭރުގައި ލިޔުއްވައިގެން ފަހު ހުށަހެޅުއްވުން އެދެމެވެ.
2·7	ބީލަން ހުށަހެޅުމަށް ހަމަޖެހިފައިވާ ތާރީޚް އެއްވެސް ސަބަބަކާހުރެ ސަރުކާރުން ބަންދު ދުވަހަކާއި ގުޅިއްޖެނަމަ ބީލަން ހުށަހެޅުން އޮންނާނީ ޖެހިގެން އަންނަ ރަސްމީ ދުވަހުގެ މި ގަޑީގައި ބަޔާންކޮށްފައިވާ ގޮތަށެވެ.

بسم الله الرحمن الرحيم

MALDIVES
INLAND REVENUE
AUTHORITY

2.8	މަސައްކަތުގެ މުއްދަތު ޖަހަންވާނީ ކަލަންޑަރު ދުވަސްތަކުގެ ގޮތުގައެވެ. އަންދާސީހިސާބު ހުށަހަޅާ ފަރާތްތަކަށް ދޭ މުއްދަތު ރަސްމީ މަސައްކަތުގެ ދުވަސްކަމުގައި އަންދާސީހިސާބުގައި ބަޔާންކޮށްފައި ވިޔަނަމަވެސް އަންދާސީހިސާބު އިވެލުއޭޝަންކުރުމުގައި މި މުއްދަތު އޮތޯރިޓީއިން ގުނާނީ ކަލަންޑަރު ދުވަސްތަކުގެ ގޮތުގައެވެ.
2.9	ބީލަން ހުށަހަޅާއިރު ފުރިހަމަ ކުރަންޖެހޭ މަޢުލޫމާތާއި ހުށަހަޅަންޖެހޭ ލިޔުންތައް ހުށަހަޅާފައި ނުވާނަމަ، ބީލަންތައް ބަލައި ނުގަނެވޭނެއެވެ. އަދި ބީލަންތައް ބަލައި ގަތުމަށްފަހުވެސް ބީލަމުގެ ކޮންމެ މަރުޙަލާއެއްގައި ނަމަވެސް ބީލަމެއް ފުރިހަމަ ނުވާކަން ފާހަގަ ކުރެވިއްޖެނަމަ، އެ ބީލަމެއް ބާޠިލު ކުރެވޭނެއެވެ. އަދި ބީލަންތައް ބަލައިގަތުމަށްފަހު ހުށަހަޅައިދީފައިވާ އަގަކީ އެކަށީގެންނުވާ އަގެއް ނަމަ، ނުވަތަ އެކަށީގެންވާ އަދަދަކަށް ބީލަން ހުށަހަޅާފައި ނުވާނަމަ، އެ ބީލަމެއް ބާޠިލުކުރުމުގެ އިޚްތިޔާރު މި އޮތޯރިޓީއަށް ލިބިގެންވެއެވެ.
2.10	މިނިސްޓްރީ އޮފް ފިނޭންސްގެ ނަންބަރު K/CIR/2019/27-13 (04 ޖުލައި 2019) މާލިއްޔަތު ސަރކިއުލަރުގައި ވާގޮތުގެމަތިން މި ބީލަމުގައި ބައިވެރިވާނީ މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓްގައި، ކުދި އަދި މެދުފަންތީގެ ވިޔަފާރި ގޮތުގައި ރަޖިސްޓްރީ ކޮށްފައިވާ ދިވެހި ވިޔަފާރިތަކަށެވެ.
2.11	ބީލަން ހުށަހެޅުމުގެ މުއްދަތު ހަމަވުމުގެ ކުރިން ބީލަމާ ގުޅޭ ކޮންމެވެސް ސުވާލެއް ބޭނުންވެއްޖެ ހިނދެއްގައި، އެކަން ލިޔުމުން (ފެކްސް/އީމެއިލް) ދަންނަވާނެއެވެ. މިގޮތުން ދަންނަވާ އެފަދަ ސުވާލުތަކަށް މަޢުލޫމާތު ކޮމިޓީގެ ބައެއްވެ. އަދި އެ ސުވާލުތަކާ ބީލަމުގައި ބައިވެރިވާ ފަރާތްތަކަށް އީމެއިލް ކުރެވިގެން ފޮނުވާނެއެވެ.

3.	އަމަލުކުރާނެ އުސޫލު
3.1	ބީލަންތައް އިވެލުއޭޓް ކުރާނީ ހަމަޖެހިފައިވާ ދެ ބައިކޮށެވެ. އެއީ ކޮލިފިކޭޝަން ކްރައިޓީރިއާ އާއި އިވެލުއޭޝަން ކްރައިޓީރިއާ މި ދެ ބައެވެ.
3.2	ކޮލިފިކޭޝަން ކްރައިޓީރިއާގައި ހިމަނާފައިވާ ކަންތައްތައް ފުރިހަމަ ނުވާ ބީލަންތައް ބާޠިލުވާނެއެވެ. އަދި މި ބީލަންތައް އިވެލުއޭޝަން މަރުޙަލާއަކަށް ނުގެންދެވޭނެއެވެ.
3.3	މިމަސައްކަތް ހަވާލުކުރާނެ ފަރާތެއް ހޮވުމުގައި ބެލޭނީ އިވެލުއޭޝަން ކްރައިޓީރިއާ އާއި އެއްގޮތަށް ޕޮއިންޓް ދިނުމުން، އެންމެ މަތިން ޕޮއިންޓް ލިބޭ ފަރާތަކަށެވެ.

بسم الله الرحمن الرحيم

MALDIVES
INLAND REVENUE
AUTHORITY

4. ބީލަންވެރިންގެ ހުންނަންޖެހޭ ޝަރުތުތައް (ކޯލިފިކޭޝަން ކްރައިޓީރިއާ)

4.1	މިމަސައްކަތް ކުރުމަށް އެދި ޕްރޮޕޯސަލް ހުށަހަޅުއްވާފައިވާ ވިޔަފާރި ރަޖިސްޓްރީ ކުރުމުގެ ޤާނޫނު (ނަންބަރު 18/2014) ގެ ދަށުން ރަޖިސްޓްރީ ކޮށްފައިވާ ފަރާތްތަކަށެވެ. ޕްރޮޕޯސަލް ހުށަހަޅުއްވާއިރު، ރަޖިސްޓްރީ ކޮށްފައިވާކަން އަންގައިދޭ ލިޔުމުގެ ކޮޕީއެއް ހުށަހަޅުއްވަން ވާނެއެވެ.

5. އިވެލުއޭޝަން ކްރައިޓީރިއާ

5.1	ބީލަން ހުށަހަޅާފަރާތްތަކުގެ ތެރެއިން އިވެލުއޭޝަން މަރުހަލާއަށް ގެންދެވޭނީ މިކަރުދާހުގެ 4 ވަނަ ނަންބަރުގައި ބަޔާންކޮށްފައިވާ ޝަރުތުތައް ފުރިހަމަވާ ފަރާތްތަކުގެ ޕްރޮޕޯސަލްތަކެވެ.
5.2	މި މަސައްކަތަށް އިވެލުއޭޝަން ކްރައިޓީރިއާގައި މާކްސް ދިނުމުގެ ތަފުސީލު، މިކަރުދާހުގެ ޖަދުވަލު 1 ގައި ތަފުސީލުކޮށް ބަޔާންކޮށްފައިވާނެއެވެ.

6. ބީލަމާއި އެކު ހުށަހަޅަންޖެހޭ ތަކެތި

6.1	ބީލަން އަގު ހުށަހަޅައިފައިވާ ކޯޓޭޝަން. މި ކޯޓޭޝަންގައި ކޯޓޭޝަން ނަންބަރު، ތާރީޚް، ތަކެތި/ޚިދުމަތް ފޯރުކޮށްދޭންޖެހޭ މުއްދަތު އަދި ސާމްޕަލް ހުށަހަޅަންޖެހޭ މުއްދަތު (ސާމްޕަލް ހުށަހަޅަން މުއްދަތު ޖަހަންޖެހޭ ބީލަންތަކަށް)، ވޯރަންޓީ ހުށަހަޅާ ތަކެތީގެ ފުލް ސްޕެސިފިކޭޝަން، ޚިދުމަތުގެ އަގު، ޖީއެސްޓީ އަދި ޖުމްލަ އަގު އެގޭން އޮތުމާއި އެކު، ސޮއިކުރުމުގެ ހުއްދަ އޮންނަ ފަރާތެއްގެ ސޮއިކުރުމާއި ވިޔަފާރީގެ ސިއްކަ ޖަހަންވާނެއެވެ. ކޯޓޭޝަންގެ ވެލިޑިޓީ މުއްދަތަކީ މަދުވެގެން 45 ދުވަސް ކަމަށްވާންވާނެއެވެ. (ކޯޓޭޝަން ހުށަހަޅުއްވަންވާނީ ކޮންމެ ލޮޓަކަށްވެސް ވަކި ކޯޓޭޝަނެއްގެ ގޮތުގައެވެ)
6.2	މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓުން ދޫކޮށްފައިވާ ވިޔަފާރި ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓްގެ ކޮޕީ
6.3	ކުދި އަދި މެދުފަންތީގެ ވިޔަފާރީގެ ގޮތުގައި ރަޖިސްޓްރީކޮށްފައިވާ ކަމުގެ ލިޔުން
6.4	ތަޖުރިބާ ލިބިފައިވާ ކަމުގެ ލިޔުން (މަސައްކަތް ކުރުމުގައި ތަޖުރިބާ ލިބިފައިވާ މުއްދަތު އެނގޭގޮތަށް) މި ލިޔުންތަކުގައި ތަޖުރިބާ ހާސިލް ކުރި ކުރުވި ފަރާތުގެ ފޯނު ނަންބަރު ހިމެނިފައިވާނެއެވެ.
6.5	ޖީ.އެސް.ޓީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓްގެ ކޮޕީ (ޖީ.އެސް.ޓީއަށް ރަޖިސްޓްރީވާން ނުޖެހޭ ފަރާތެއްނަމަ މި އޮތޯރިޓީން ދޫކޮށްފައިވާ ޓެކްސްޕޭޔަރ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓް/ ޓީއައިއެން ސެޓްފިކެޓްގެ ކޮޕީ)
6.6	މި އޮތޯރިޓީން ދޫކޮށްފައިވާ ޓެކްސް ކްލިއަރެންސް ރިޕޯޓް (ދޫކުރިތާ 3 މަސް ހަމަނުވާ)

6.7	ބީލަމުގެ އަގު -/500,000 (ފަސް ލައްކަ ރުފިޔާ) އަށްވުރެ ބޮޑުނަމަ، ޤަވާއިދުގައިވާގޮތަށް ބީޑް ސެކިއުރިޓީގެ ގޮތުގައި -/25,000 (ފަންސަވީސް ހާސް ރުފިޔާ) ގެ ބީޑް ސެކިއުރިޓީ ޑޮކިއުމަންޓް ހުށަހަޅަންވާނެއެވެ. ބީޑް ސެކިއުރިޓީގެ ވެލިޑިޓީ މުއްދަތަކީ މަދުވެގެން 60 ދުވަސް ވާންވާނެއެވެ. (ބޭންކް ނުވަތަ ފައިނޭންޝަލް އިންސްޓިޓިއުޝަނެއްގެ ގެރެންޓީ ލިޔުން ޤަބޫލުކުރެވޭނެއެވެ، ބޭންކް ޗެކް ނުވަތަ ނަގުދު ފައިސާ ޤަބޫލު ނުކުރެވޭނެއެވެ)
7.	**ބީލަން ކާމިޔާބުވުން**
7.1	ބީލަމުގެ އިވެލުއޭޝަން ކުރުމަށްފަހު ބީލަން ކާމިޔާބު ކުރި ފަރާތަށް އަދި ބީލަމުގައި ބައިވެރިވި އެހެން ފަރާތްތަކަށް ބީލަން އެވޯޑް ކުރެވުނުކަން މި އޮފީހުން އަންގާނެއެވެ.
7.2	ބީލަން އެވޯޑްކުރިކަން އެންގުމަށްފަހު ހުރިހާ ބީލަންވެރިންނަށް މި ނިންމުމާމެދު އިއުތިރާޟްކުރާނަމަ އެކަން މި އޮފީހަށް ހުށަހެޅުމުގެ ފުރުސަތު 05 (ފަހެއް) ދުވަހުގެ މުއްދަތެއް ދެވޭނެއެވެ. މިގޮތުން ހުށަހަޅާ އިއުތިރާޟްތައް ހުށަހަޅަންވާނީ ލިޔުމުންނެވެ.
7.3	7.2 ގައިވާ މުއްދަތުގެ ތެރޭގައި އެއްވެސް ބީލަންވެރިއެއްގެ އިއުތިރާޟެއް ލިބިފައި ނުވާނަމަ ބީލަން ކާމިޔާބު ކުރި ފަރާތަށް މަސައްކަތުގެ އެއްބަސްވުމުގައި ސޮއިކުރަން ހުށަހެޅޭނެއެވެ. އެއްބަސް ވުމުގައި ސޮއިކުރަން ހުށަހަޅާ ތާރީޚުން ފެށިގެން 03 (ތިނެއް) ދުވަހުގެ މުއްދަތުގެ ތެރޭގައި އެއްބަސްވުމުގައި ސޮއި ކުރަން ޖެހޭނެއެވެ.
7.4	ބީލަމުގެ އަގު -/500,000ރ (ފަސް ލައްކަ ރުފިޔާ) އަށް ވުރެ ބޮޑުނަމަ ބީލަން ކާމިޔާބުކުރާ ފަރާތުން އެގްރީމެންޓުގައި ސޮއިކުރުމުގެ ކުރިން މާލިއްޔަތު ޤަވާއިދުގައިވާގޮތަށް ޕާރފޯމަންސް ގެރެންޓީ ގެ ގޮތުގައި އަގުގެ 5% ހުށަހަޅަންޖެހޭނެއެވެ. މި ޕާރފޯމަންސް ގެރެންޓީ ބީލަން ކާމިޔާބު ކުރިކަން އަންގާ ތާރީޚުން ފެށިގެން ރަސްމީ ބަންދު ދުވަސްތައް ނުހިމަނައި 05 (ފަހެއް) ދުވަހުގެ ތެރޭގައި ހުށަހަޅަން ވާނެއެވެ. އަދި ޕާރފޯމަންސް ގެރެންޓީގެ ވެލިޑިޓީ މުއްދަތަކީ މަދުވެގެން ޑެލިވަރީގެ މުއްދަތު އިތުރުން 30 ދުވަސް ވާންވާނެއެވެ. (ބޭންކް ނުވަތަ ފައިނޭންޝަލް އިންސްޓިޓިއުޝަނެއްގެ ގެރެންޓީ ލިޔުން ޤަބޫލުކުރެވޭނެއެވެ، ބޭންކް ޗެކް ނުވަތަ ނަގުދު ފައިސާ ޤަބޫލު ނުކުރެވޭނެއެވެ)
7.5	މަސައްކަތް ފެށުމަށް ހުއްދަ ދޫކުރެވޭނީ އެއްބަސްވުމުގައި ސޮއިކުރުމަށްފަހުގައެވެ.
7.6	މަސައްކަތުގެ މުއްދަތު ގުނަން ފަށާނީ މަސައްކަތް ކުރުމަށް މި އޮފީހުން ހުއްދަދީ އެއްބަސްވުމުގައި ސޮއިކުރާ ތާރީޚުން ފެށިގެންނެވެ. އެހެންނަމަވެސް ޕާރފޯމަންސް ގެރެންޓީ ހުށަހަޅަންޖެހޭ ހާލަތުގައި، ބީޑް ކާމިޔާބު ކުރިކަން މި އޮފީހުން އެންގުމަށްފަހު ޕާރފޯމަންސް ގެރެންޓީ ގެނައުމަށް މި އުސޫލުގެ 7.4 ވަނަ މާއްދާއިން ދީފައިވާ މުއްދަތުގައި ގެރެންޓީ ނުގެނެސް ލަސްވާ ދުވަސްތައް މަސައްކަތުގެ މުއްދަތުގެ ގޮތުގައި ހިމަނައިފައިވާ ދުވަސްތަކުން އުނިކުރުމުގެ އިޚްތިޔާރު މި އޮފީހަށް ލިބިގެންވެއެވެ.
7.7	7.3 ގައިވާ މުއްދަތުގައި މަސައްކަތުގެ އެއްބަސްވުމުގައި ސޮއި ނުކޮށްފިނަމަ، އަދި 7.4 ގައިވާ މުއްދަތުގައި ޕާރފޯމަންސް ގެރެންޓީ ހުށަހަޅައިނުދީފިނަމަ، ބީލަން އެވޯޑްކުރިކަން މި އިޢުލާނުން ނިސްބަތުން ބާތިލްކޮށް ދެވަނައަށް ކާމިޔާބުވި ފަރާތަށް މަސައްކަތް ހަވާލުކުރެވޭނެއެވެ.

بسم الله الرحمن الرحيم

MALDIVES
INLAND REVENUE
AUTHORITY

ޖަދުވަލު 1: ހުށަހަޅަންޖެހޭ ލިޔުންތައް

ހުށަހަޅަންޖެހޭ ލިޔުންތައް			
	6.1	ހުށަހަޅާ އެސްޓިމޭޓް (ކޯޓޭޝަން) (ކޯޓޭޝަން ހުށަހަޅުއްވަންވާނީ ކޮންމެ ލޮޓަކަށްވެސް ވަކި ކޯޓޭޝަނެއްގެ ގޮތުގައެވެ)	1
	6.2	ކުންފުނި/ޕާޓްނަރޝިޕް/ ކޯޕަރޭޓިވް ސޮސައިޓީ/ އަމިއްލަ ފަރުދުންގެ ވިޔަފާރީގެ ރަޖިސްޓްރީގެ ކޮޕީ	2
	6.3	ކުދި އަދި މެދުފަންތީގެ ވިޔަފާރީގެ ގޮތުގައި ރަޖިސްޓްރީކޮށްފައިވާކަމުގެ ލިޔުން	3
	6.5	ޖީއެސްޓީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓް ކޮޕީ (ޓެކްސް ޕޭޔަރ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓް/ ނޮޓިފިކޭޝަންގެ ކޮޕީ.)	4
	6.6	ޓެކްސް ކްލިއަރަންސް ރިޕޯޓުގެ ކޮޕީ (ދޫކުރިފަހުން 3 މަސް ހަމަނުވާ).	5
	6.7	ބިޑް ސެކިއުރިޓީގެ (ބިޑް ސެކިއުރިޓީގެ ހުށަހަޅަންޖެހޭ ޕްރޮޖެކްޓްތަކަށް)	6

ޖަދުވަލު 2: ބިޑް ސެކިއުރިޓީ (ބޭންކް ގެރެންޓީ) ނަމޫނާ

Whereas, ……………………………………………..*[name of Bidder]* (hereinafter called “the Bidder”) has submitted his Bid for the Project no……….issued by the Maldives Inland Revenue Authority on ……………………………… …………..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,

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.

* 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.

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]

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

MALDIVES
INLAND REVENUE
AUTHORITY

ޖަދުވަލު 3: މަސައްކަތުގެ ތަފްސީލް

Required Item: Web Application Firewall
Quantity: 1

SPECIFICATIONS

S. No.	Item	Technical Specifications
1	**Industry Certifications and Evaluations**	
	1.1	The OEM should be in the Gartner's Leaders Magic Quadrant for "Web Application Firewall" for any one year in the last ten published reports.
	1.2	The Solution should meet PCI DSS Compliance as per PCI DSS requirement and should provide reports for PCI DSS compliance.
2	**Architecture and Performance**	
	2.1	Proposed solution should be a dedicated Appliance based solution with appliance height not more than 1 U.
	2.2	Platform should be a full proxy architecture
	2.3	The Operating system of proposed appliance should be default Deny and should not allow communication between two ports without explicit configuration
	2.4	The proposed Appliances should support LEDs / LCD screen to provide status on CPU and Memory utilization of appliance as well as management interface configuration
	2.5	The proposed appliance should have minimum 4 x 1G Copper ports and 2 x 10 GE SFP+ fiber port populated
	2.6	The proposed appliance should provide minimum throughput of 10 Gbps
	2.7	The solution should support up to 125k L4 connections per second and 350K L7 requests per second
	2.8	The proposed appliance must support minimum SSL TPS of 2.5Kk (RSA 2k keys) and minimum 2.1K (with ECDSA 256 key).
	2.9	OS should be default deny and should be certified by ICSA
	2.10	Should have a HDD with minimal capacity of 500 GB
	2.11	The Appliance must have minimum 16 GB RAM
	2.12	Should have dual power supply
	2.13	The proposed appliance should support minimum 3Gbps of compression throughput.
	2.14	The proposed appliance should support minimum 5 Gbps of SSL throughput
	2.15	The product should comply and support IPv4 and IPv6 both and NAT64
	2.16	Proposed WAF instance should be configurable in such a way that multiple network zones can be configured without sharing the data between them and without any compromise of security.
	2.17	The goods must be support dual-stack (IPv4 and IPv6) operation across all features

	2.18	Should have full support IPv6. It should support all IPv6 scenarios: a. IPv4 on the inside and IPv6 on the outside b. IPv6 on the inside and IPv4 on the outside c. IPv6 on the inside and outside
	2.19	Platform should be a full proxy architecture and must perform reverse proxy for inside applications for HTTP/HTTPs, PCoIP and DNS
	2.20	Should have a dedicated out-of-band Ethernet management port
	2.21	Should support VLAN, LACP & Trunking
	2.22	Should support anit-DDoS, DNS, and SSL-VPN along with SSO and OTP (Generation + Verification) as and when required with additional license.
	2.23	Proposed solution should support Fraud Protection on same appliance with additional license as and when required, with following features: a) Application Level Encryption - encrypting username and password b) Encrypting user's key stroke with Private-Public Key combination c) Should be able to identify and prevent automated payments and money transfers initiated by malware or bots d) Should performs a series of transaction checks—including behavioral analysis, signature and function verification
	2.24	The proposed model should be scalable to support the following optional additional features to ensure application security and business continuity with licenses as below with additional cost: Remote Access via SSL VPN & SSO Solution - To control & secure user access of Internal Applications Global Server Load Balancing - To load balance the traffic across multiple sites based on Geo location, latency and other metrics DNS Firewall - To protect from dns based attacks DDoS Protection - To protect against L4 DDoS attacks
3	**Security Requirements**	
	3.01	Validation should be performed on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.
	3.02	When deployed as a proxy (either a transparent proxy or a reverse proxy), the Web application firewall should be able to digitally sign cookies, encrypt cookies, and to rewrite URLs.
	3.03	The Proposed WAF Solution should support both a Positive Security Model and a Negative Security Model. OEM should provide regular update for CVE signatures. OEM should have Security Incident Response team
	3.04	Auto-learn options should be available to tweak and fine tune rules. The auto learn policy should have provision to put into staging mode for specific time period to avoid the false positive.

	3.05	The solution must be able to block transactions with content matching for known attack signatures while allowing everything else.
	3.06	The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Whitehat Sentinel, IBM Appscan, HP Webinspect, Rapid7 and QualysGuard, for rapid virtual patching.
	3.07	Should be able to import Vulnerability scanner report from Whitehat Sentinel, IBM Appscan, HP Webinspect, Rapid7 and QualysGuard and fixed those vulnerabilities within the waf using xml file.
	3.08	The solution must support both URL rewriting and content rewriting for http header and body when it is deployed in the reverse proxy mode.
	3.09	Solution should support API security including support for uploading swagger file.
	3.1	The solution must be able to validate encoded data in the HTTP traffic.
	3.11	The solution must be able to identify Web Socket connections and provide security for WebSocket including exploit against Server abuse, login enforcement, XSS and SQL injection.
	3.12	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection\learning mode.
	3.13	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.
	3.14	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.
	3.15	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.
	3.16	The Proposed WAF Solution should have capability to mitigate, learn and adapt to unique application layer user interaction patterns to enable dynamic defenses based on changing conditions
	3.17	The Proposed WAF Solution should have Correlated Attack Validation capability or Correlation features which examines multiple attributes such as HTTP protocol conformance, profile violations, signatures, special characters, and user reputation, to accurately alert on or block attacks and also to eliminate false positives.
	3.18	The Proposed WAF Solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.
	3.19	The Proposed WAF Solution Should support ICAP integration with other security devices for file scanning.

	3.20	The proposed WAF Solution should be configured with real-time threat intelligence on known malicious sources, such as: • Malicious IP Addresses: Sources that have repeatedly attacked other websites • Anonymous Proxies: Proxy servers used by attackers to hide their true location • TOR Networks: Hackers who are using The Onion Router (TOR) to disguise the source of attack • IP Geolocation: Geographic location where attacks are coming from and block access • Phishing URLs: fraudulent sites (URLs) that are used in phishing attacks • Comment Spammers: IP addresses of known active comment spammers
	3.21	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript, Image and Sound CAPTCHA challenges. This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot.
	3.22	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behavior analysis, reverse DNS lookup
	3.23	The Web Application Firewall should have "Anti-Automation" protection which can block the automated attacks using hacking tools, scripts, frame work etc.
	3.24	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack.
	3.25	Solution should support Behavioral L7 DDoS mitigation to detect attacks without human intervention
	3.26	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page
	3.27	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks
	3.28	The Proposed WAF Solution should Identify and limit / block suspicious clients , headless browsers and also mitigate client side malwares
	3.29	The Proposed WAF Solution should protect API based communication between client & servers using all the relevant WAF signatures.
	3.30	Should provide encryption for user input fields to protect from browser based malwares stealing users credentials
	3.31	Should support Websocket Security Inspection
4	**Deployment and Operational Requirements**	
	4.01	Solution should have the ability to build a base/parent policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings

	4.02	The Proposed WAF Solution must support deployment as inline proxy, one arm mode or transparent bridge mode.
	4.03	On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address. For particularly destructive attacks, the Web application firewall should be able to block the user or the IP address for a configurable period of time.
	4.04	The solution must allow administrators to add and modify signatures.
	4.05	The solution must support regular expressions for the following purposes: - Signatures definition - Sensitive data definition - Parameter type definition - Host names and URL prefixes definition - Fine tuning of parameters that are dynamically learnt from the web application profile
	4.06	The WAF instance should have option to enable x-forwarder option per service to log actual client IP in webserver logs even deployed in Reverse Proxy mode.
	4.07	The proposed solution should support min 4000 contexts or partitions or multiple profiling separately for each application without any additional license.
	4.08	Separate policies should be applied for different applications configured on the same WAF
	4.09	The solution should have pre-built templates for well-known applications eg Microsoft Sharepoint, OWA, ActiveSync, SAP, Oracle Applications/Portal, PeopleSoft, Lotus Domino .
	4.10	All web facing applications are to be integrated to WAF without any limitation on the number of application. Solution should support the deployment modes based on application needs
	4.11	Proposed Solution should have ability to stage rule or signature before final deployment. During staging period false positive events for corresponding rules and signatures can be managed and adjusted to match real world app data.
	4.12	Proposed Solution should have ability to fallback to another host in case then protected App is not available or return HTTP error codes
	4.13	Proposed Solution should have ability of HTTP response logging.
	4.14	Proposed Solution should have ability to automatically detect software technology used on backend side to define signature sets required for defined Proposed Solution policy.
	4.15	Proposed Solution should have ability to configure meta characters sets per parameter or header.
	4.16	Proposed Solution should have ability to configure way to analyze request payload based on custom rules for each URL entry configured in the security policy
	4.17	Proposed Solution should track request length, URL length, POST data length based on request file type.

	4.18	Proposed Solution should have ability to adjust parameters of automatic learning engine/ machine learning in WAF to define speed and accuracy of learning
	4.19	Application Security solution should offer protection for FTP and SMTP protocols.
	4.20	Solution should support user-written scripts, irules, that provide flexibility to control application flows
	4.21	Proposed Solution Attack log entry should have action to accept further request like this in policy or reject such an attack in future.
	4.22	Proposed Solution should have configuration of anti-bot browser challenge action. IT should be either sent before access to backend, during access to backend or disabled.
	4.23	Proposed Solution should have ability to differentiate DoS mitigation action based on Attacker Source IP, device fingerprint, URL or Geolocation.
	4.24	Proposed Solution should have ability dynamically generate signatures for L7 DoS attacks. These signatures should be exportable for use on 3rd party systems.
	4.25	Proposed Solution should have ability to define new custom types of attack based on custom events
	4.26	Proposed Solution should be able to track application changes over time and adjust config elements and rules based on that data.
	4.27	Proposed solution should be able to track unused elements in the policy and suggest to remove them after a specified period of time
	4.28	Should support Integrated Web Application Load balancing that helps to reduce latency and gives singular window of management. WAF & Load balancer should be on the same virtual instance
	4.29	Solution should support below load balancing algorithm: Round Robin Ratio (member) Least Connections (member) Ratio (node) Least Connections (node) Weighted Least Connection (member) Weighted Least Connection (node) Ratio Least Connection (member) Ratio Least Connection (node)
	4.30	Solution should support below persistency methods: Cookie Persistency Source Address Host Destination Address

	4.31	Solution should support below monitors: FTP, Gateway ICMP, HTTP, HTTPS, ICMP, SOAP, TCP, TCP Half Open, UDP
	4.32	The proposed model should be scalable to support the following optional additional features to ensure application security and business continuity with licenses as below with additional cost: Remote Access via SSL VPN & SSO Solution - To control & secure user access of Internal Applications Global Server Load Balancing - To load balance the traffic across multiple sites based on Geo location, latency and other metrics DNS Firewall - To protect from dns based attacks DDoS Protection - To protect against L4 DDoS attacks
5		**Load Balancing**
	5.01	Should support configurable TCP/IP queuing and buffering
	5.02	Should have application delivery features such as layer 7 load balancing, layer 7 content switch, caching, hardware based SSL offload and server side compression
	5.03	Should have capability to monitor the applications using intelligent application level monitors which can be system defined, internal or external executable scripts
	5.04	Should be able to tune monitoring frequency and time automatically when server is available for long time, this is to avoid monitoring load on server
	5.05	Should have 2048 and 4096 bit key for SSL certificate support
	5.06	Should have capability to support ECC, RSA and ECC+RSA (Hybrid) Certificates for SSL offload
	5.07	Should provide static and dynamic load balancing algorithms such as round robin, weighted round robin, fastest, predictive and observed
	5.08	Should be application aware and provide Full Proxy for protocols such as HTTP, HTTPS, FTP, SIP, DNS, Diameter, RADIUS etc.
	5.09	Should support inspection of SSL traffic for reverse proxy and forward proxy deployment. Should also support ICAP interface for integration with external security systems.
	5.10	Should support IoT Device authentication over SSL and MQTT Message parsing and MQTT load balancing.
	5.11	Should have HTTP 2.0 gateway in environment where the client to load balancer traffic is HTTP 2.0 and from load balancer to server is normal HTTP 1.1

	5.12	Should support web content delivery acceleration by modifying the data and reducing the number of round trips required to fully display a web page
	5.13	Should support different algorithm for reducing round trips: 1, Content reordering 2, Content inlining 3, Image optimization 4, Minification 5, Multi-protocol optimizations (HTTP, FTP, MAPI, UDP)
	5.14	Should support same version and configuration when load balancer is migrated to cloud like AWS, Azure, Rackspace, dimension data
	5.15	Should support SDN integration with Cisco ACI, Vmware NSX and RedHat Openstack
	5.16	The proposed appliance shall have iApps template for ease of deployment.
	5.17	The proposed solution must be able to load balance both TCP and UDP based application from L2 to L7 and full proxy for lightweight message queue protocol for machine to machine connectivity between IoT appliances such as small sensors, mobile devices etc..
	5.18	The proposed solution must be able to perform TCP multiplexing and TCP optimization, SSL Offloading with SSL session mirroring and persistence mirroring, hardware based compression, caching etc in active-passive mode.
	5.19	The proposed solution must offer out of band programming for control plane along with data plane scripting for function like content inspection and traffic management
	5.20	Server Load Balancer should support SQL-based querying for the following databases for health checks: • Oracle • MSSQL • MySQL • PostgreSQL • DB2
	5.21	Proposed solution should provide SSL offloading with the SSL connection and persistence mirroring during the HA failover
	5.22	The proposed solution must support policy nesting at layer4 and layer7 to address the complex application integration. Further it should also provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..
	5.23	The Proposed load balancer should support TLS 1.0, TLS 1.2, TLS 1.3 with 2048 Bit SSL encryption
6	**Integration**	
	6.1	Proposed solution should be able to integrate with external SSL visibility solution
	6.2	Proposed solution should also integrate with SIEM
	6.3	The solution should also support sending of logs in CEF standard
7	**Administration and Management**	
	7.1	Management solution should support Role-Based Access Control or multiple user roles that facilitate separation of duties. i.e. Administrator (Super-User), Manager, SSL Certificate Manager

	7.2	Proposed solution should support multiple administration domains (or partitions) to configure and administer the system. This would include support for using remote authentication servers (e.g. LDAP, Windows AD, RADIUS and TACACS+) to store system user accounts.
	7.3	Proposed solution should provide account creation with access level that can - Provides User roles that can be assigned such as Administrator, Resource Administrator, User Manager, Manager, Application Editor, Application Security Policy Editor, Operator, Script Editor or Guest. It can be no access for user account to system resources - Provide administrative partition where it limit user access to certain device objects which include entities that user accounts can manage and place in administrative partition.
	7.4	Proposed Solution should have Role-based management with user authentication. There should be web application security administrator whom has access to web security policy objects in web profile, modify web profiles but cannot create or delete those profiles, and web application security editor whom configure or view most parts of the web security policy object in specific controlled partition holding the policy and profile objects.
	7.5	The solution should support the following authentication mechanism for accessing the solution In-built authentication in the solution - Kerberos authentication - LDAP authentication - RADIUS authentication
	7.6	Organization should be able to deploy or remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.
	7.7	Should provide HTTPS interface management for administering the device
	7.8	Should provide SSH interface management for administering the device
	7.9	Should provide troubleshooting and traffic analysis tool like tcpdump
8	**Reporting**	
	8.1	Reporting and logging of all HTTP data and the application level including HTTP headers, form fields, and the HTTP body.
	8.2	Support proper Reporting and Logging facilities.
	8.3	Should be able to report events via standard mechanisms, for example, to a syslog or SNMP server or a SIEM solution.
	8.4	The solution must support generation/ both predefined as well as custom-built reports as per Organization's requirements with both tabular views, pdf and data analysis graphical views.
	8.5	Should provide historical graphical reporting for the last 30 days on appliance itself
	8.6	Should have a built-in tool to take a snapshot of the unit for troubleshooting and analysis purpose

	8.7	Vendor should provide a service to upload this snapshot and get feedback on the health of the unit & missing Hotfixes and best practices
	8.8	Solution should have the option to classify the bad or suspected bot type and provide detailed dashboard based on the bad/suspected BOT types
	8.9	The solution must have an integrated dashboard containing various features of alert and report generation including : a. CPU Usage b. Memory Usage c. Connections Statistics d. Throughput Statistics (Client Side and Server Side throughput) e. Virtual Server Status f. Application services Status g. Application Server Status
	8.10	Should have a Reporting Engine built-in
	8.11	Should support High Speed Logging to a syslog server
	8.12	Support for customized logging through scripts to log any parameter from L3 to L7, like Geolocation, IP addresses, client browser, client OS, etc..
	8.13	Should support integration with SIEM tools like Arcsight and Splunk
	8.14	Should have a log publisher to publish logs to multiple log destinations for the same application (or virtual server)
	8.15	Should have a filtering capability before publishing to a log destination
	8.16	Should provide historical graphical reporting on the same device
	8.17	Should provide Dashboard with Guided steps for OWASP Top 10 protection
9	**Support**	
	9.1	OEM of the Proposed Solution Vendor should provide regular updates to geo-location database from their public downloads website
	9.2	OEM should have a Technical Assistance Center (TAC) which Follow the Sun Model with toll free numbers

Special Instruction to Bidding Parties: -

- Should provide on the job training for 2 staff
- Should provide overseas training for 2 staff
- Should include support for 1 year
- Bidder should submit authorization letter from Vendor
- Should provide a schedule of implementation

Evaluation Criteria

Price: 100%
Delivery Period: Must be delivered within a maximum of 30 days