ބީލަމުގެ މަޢުލޫމާތު ކަރުދާސް

ޕްރޮޖެކްޓްގެ ނަން:	އެޑްވާންސްޑް އެންޓި ޕްރިންޓް ޕްރޮޖެކްޝަން ސްކްރީން ޕްރޮކިއުމަންޓް ފަރާތަކުން ހޯދުން
ޕްރޮޖެކްޓްގެ ނަންބަރު:	38/2026/W-025
އިޢުލާން ނަންބަރު:	(IUL)38-AB/38/2026/720
އިޢުލާން ތާރީޚް:	11 ޖޫން 2026

ބީލަން ހުށަހަޅަންޖެހޭނީ:

ތަން:	އިލެކްޝަންސް ކޮމިޝަން، 5 ވަނަ ފަންގިފިލާ، ޕީ.އޭ ކޮމްޕްލެކްސް، ހިލާލީމަގު، މާލެ.
ތާރީޚް:	21 ޖޫން 2026
ގަޑި	10:30

އިލެކްޝަންސް ކޮމިޝަން

މާލެ، ދިވެހިރާއްޖެ

ބީލަން ހުށަހަޅާ ފަރާތްތަކަށް ދެވޭ އިރުޝާދު

1. ތައާރަފު

މި ކަރުދާހުގައި ހިމެނޭ ގަންނަން ބޭނުންވާ މުދަލާއި ހިދުމަތުގެ މައުލޫމާތާއި، ބީލަން ހުށަހަޅާނެ ގޮތުގެ އުސޫލުތަކާއި، ބީލަންވަޒަންކުރާނެ ގޮތުގެ އިރުޝާދުދެވެ.

2. ބީލަމަށް ކުރިމަތިލެވޭނީ ފަރާތްތަކުގައި ހުންނަންޖެހޭ ޝަރުތުތައް

2.1 ބީލަން ހުށަހަޅާފަރާތަކީ، ވިޔަފާރި ރަޖިސްޓްރީ ކުރުމުގެ ޤާނޫނު (ޤާނޫނު ނަންބަރު: 2014/18) ގެ ދަށުން ވިޔަފާރި ރަޖިސްޓްރީ ކުރެވިފައިވާ ތިރީގައި ބަޔާންކުރާ ފަރާތްތަކަށެވެ. އަދި މި ބީލަމުގެ އެންމެހައި ކަންތައްތައް ކުރިއަށްދާނީ ދައުލަތުގެ މާލިއްޔަތު ގަވާއިދުގައި ބަޔާންކޮށްފައިވާ ހަމަތަކާއި އުސޫލުތަކުގެ މަތިންނެވެ.

2.1.1 ދިވެހިރާއްޖޭގެ ކުންފުންޏާއިބެހޭ ޤާނޫނުގެ ދަށުން ރަޖިސްޓްރީ ކުރެވިފައިވާ ކުންފުންޏެއް.

2.1.2 ޕާޓްނަރޝިޕްގެ ޤާނޫނުގެ ދަށުން ރަޖިސްޓްރީ ކުރެވިފައިވާ ޕާޓްނަރޝިޕެއް.

2.1.3 ކޯޕަރޭޓިވް ސޮސައިޓީގެ ޤާނޫނުގެ ދަށުން ރަޖިސްޓްރީ ކުރެވިފައިވާ ކޯޕަރޭޓިވް ސޮސައިޓީއެއް.

2.1.4 އަމިއްލަ ފަރުދުންގެ ވިޔަފާރީގެ ޤާނޫނުގެ ދަށުން ރަޖިސްޓްރީ ކުރެވިފައިވާ އަމިއްލަ ފަރުދުންގެ ވިޔަފާރިއެއް.

2.2 މިފަދައިން 2.1 ގައި ބަޔާންކުރާ ފަރާތްތަކުގެ ތެރެއިން މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓުގެ ކުރީ އަދި މިހާރުގެ ވިޔަފާރީގެ ޑިޕާޓްމަންޓުގައި ރަޖިސްޓްރީ ކުރެވިފައިވާ ދިވެހިވިޔަފާރިއެއް

2.3 މީގެ އިތުރުން ބީލަން ހުށަހަޅާ ފަރާތަކީ، ދައުލަތުގެ މާލިއްޔަތުގެ ގަވާއިދުގެ 17 ވަނަ ބާބުގައިވާގޮތުގެ މަތިން ދައުލަތުގެ ބީލަމުގައި ބައިވެރިވުމުގެ ފުރުޞަތު ސަސްޕެންޑްކުރެވިފައިވާ ފަރާތަކަށް ނުވުން.

3. މައުލޫމާތު ސާފުކުރުން

ބީލަމާއި ގުޅިގެން ސާފުކުރަންޖެހޭ މައުލޫމާތެއް ވާނަމަ ޕްރޮކިއުމަންޓް، މައުލޫމާތު ސާފުކުރުމަށް ދެވިފައިވާ މުއްދަތުގެ ތެރޭގައި procurement@elections·gov·mv: މި އީމެއިލް އެޑްރެހަށެވެ. އަދި ގުޅުއްވާނީ 3004461 ނުވަތަ 3004428 އަށެވެ.

4. ބީލަން ތައްޔާރުކުރުން

4.1 **ބީލަމުގައި ބޭނުން ކުރާ ބަސް:-** ބީލަން ހުށަހަޅާ ފަރާތުން ބީލަން ތައްޔާރު ކުރަންވާނީ ބީލަމާއެކު ދިވެހިބަހާއި ނުވަތަ އިނގިރޭސިބަހުންނެވެ. އަދި ބީލަމާއެކު ހުށަހަޅަންޖެހޭ ރިފަރެންސް ލިޔުންތައް އިނގިރޭސި ބަހުން ހުށަހެޅިދާނެއެވެ.

4.2 **ބީލަމުގައި ބޭނުން ކުރާ ފައިސާ:-** މި ބީލަމުގައި އަގު ކުރުވިފައި ހުންނަންވާނީ ދިވެހި ރުފިޔާއިން ޖީއެސްޓީއަށް ދައްކާ އަދަދު ހިމަނައިގެންނެވެ.

4. ބިލް ތައްޔާރުކުރުން

4.3 **ބިލްގެ މުއްދަތު:-** ބިލްގެ މުއްދަތަކީ ހަމަވާ ތާރީޚް އިންވޮއިސް ބިލް ހުށަހަޅާ ތާރީޚުން ފެށިގެން 120 ދުވަހުގެ މުއްދަތުގައެވެ.

4.4 ބިލްގެ ހުރިހާ ސަފްޙާއެއްގައި ބިލް ހުށަހަޅާ ފަރާތުގެ ނަމާއި އެފަރާތުން ކުރާ ފަރާތުގެ ސްޓޭމްޕް ކުންފުނީގެ ތައްގަނޑު އަދި ހުރިހާ ސަފްޙާއެއްގައި ތަރުތީބުން ނަންބަރު ޖަހަންވާނެއެވެ.

5. ބިލް ހުށަހެޅުން

5.1 ބިލް ހުށަހަޅާނީ ސީދާ އިދާރާގައި ބަންދުކުރެވިފައެވެ. ސީދާ އިދާރާގެ ބޭރުގައި ހުށަހަޅާ ފަރާތުގެ ނަމާއި ކޮންޓްރެކްޓް ހުށަހަޅާ ބިލްތަކުން އެނގެން އޮންނަންވާނެއެވެ.

5.2 ޖީ.އެސް.ޓީ ނަގާ މުދަލާއި / ޚިދުމަތްތަކަށް އަގު ހުށަހަޅަންވާނީ ޖީ.އެސް.ޓީ ހިމަނައިގެން ދިވެހި ރުފިޔާއިންނެވެ. ހުށަހަޅާ ބިލްގައި އަގުތައް ސާފުކޮށް އެނގެން އޮންނަންވާނެއެވެ. އަދި ހުށަހެޅުމުގައި ދެވިފައިވާ ހުރިހާ ބައިތަކެއް އަދި ހުށަހަޅަންވާނެއެވެ.

5.3 ބިލް ހުށަހެޅުމުގައި ކަނޑައެޅިފައިވާ ގޮތް ފާއިތުވުމުން ހުށަހަޅާ އެއްވެސް ބިލެއް ބަލައި ނުގަނެވޭނެއެވެ. ބިލްތަކުގައި ބަޔާންކޮށްފައިވާ އަގު ކަނޑައެޅުން ހަމަޖެހިފައިވާ އެކަމަށް ކަނޑައެޅިފައިވާ ގޮތުގައި ބިލް ހުށަހަޅާ ހުރިހާ ފަރާތްތަކަށް ހާމަކުރަންވާނެއެވެ. ބިލް ހުށަހެޅުމަށްފަހު، އަގަށް ބަދަލެއް ނުގެނެވޭނެއެވެ. ބިލް ހުށަހަޅާ ކަނޑައެޅިފައިވާ ގޮތް ޤަވާޢިދުގެ ކުރިން ހުށަހަޅާ ކަނޑައެޅިފައިވާ މުއްދަތާއި ގޮތް ކަމަށްވާ ކުރުމަށް ބިލް ހުށަހަޅާ ފަރާތުގެ ޒިންމާއެކެވެ.

5.4 ބިލް ހުށަހަޅާ ފަރާތުން ކަނޑައެޅިފައިވާ ގޮތަށް ހިސާބުވާން ވާނެއެވެ. އަދި މިގޮތުން ހުށަހަޅާ ބިލްތަކާ ގޮތުން މައުލޫމާތު ސަޕްލަޔަރުން ބޭނުންކޮށްގެން ހިނގުމުގައި އެކަމަކާ މައުލޫމާތު ދޫކުރާތީ މިކަމާ ހިސާބުވާން ވާނެއެވެ. ބިލް ހުށަހެޅުމުގެ ކުރިން ހިމާޔަތް އެފަދަ ނުވަތަ އޮޑިޓަރ ޢަދުލުވެރި ކަމާ ސަޕްލަޔަރުން ބޭނުންވާ ބަޔާން ސަޕްލަޔަރުން ބޭނުންވާނެއެވެ. ބިލް ހުށަހެޅުމަށް ހިސާބު ކުރުވާ ފަހަތަކުން ހުށަހެޅުމާ އެކުގައި ބިލްކުރެވޭ.

5.5 މިބާވަތުގައި ގޮތުގެން އިލެކްޓްރޯނިކް ޓްރާންސްފަރ އެކައުންޓްނަންބަރު ދޫކުރަމަ އެ އެކައުންޓްނަންބަރު ޓްރާންސްފަރގެ ފޯމް އަދި ބޭންކުގައި ބެލެންސް ޚާއްޞަ ކުރެވޭނެއެވެ.

5.6 އިންވޮއިސްކުރެވޭ ޚިދުމަތް/މުދަލުގެ ޙަވާލާ، މި އިދާރާއިން ބޭނުން ނުވާނެ ރިސީޓްގައި އެކަމުން ބިލްތަކަށް ބޭނުންވާ ކުރުމުގެ އިންވޮއިސްގައި މިދާއިރާގެ ވިޔަފާރިވެއެވެ. މިގޮތުން ބިލްތަކަށް ބޭނުން ކުރުވާ ބިލްތަކަށް އެންމެ އާންމުކޮށް އިންވޮއިސްކުރަންވާނެއެވެ.

6. ބެލަން ބާޠިލުކުރުން

6.1 މި މާއްދާގައި ބަޔާންކޮށްފައިވާކަމެއް ފުރިހަމަ ނުވާނަމަ އެ ބެލަމެއް ބާޠިލު ކުރެވޭނެއެވެ.

6.1.1 އެނެކްސް 1 (މަޢުލޫމާތު ކަރުދާސް)ގައި ބަޔާންކޮށްފައިވާ ގޮތަށް ބެލަން ހުށަހަޅާފައިނުވުން.

6.1.2 އެނެކްސް 3 (އަގުގެ ހުށަހަޅާ ކަރުދާސް)ގެ ޖުމްލަ އަގާއި ހުށަހަޅާ އެސްޓިމޭޓް (ކޮޕީ ސްކޭން، ބީ.އޯ.ކިއު. ނުވަތަ އަސްލާސް ރިޕޯޓް) ޖުމްލަ އަގު ދިމާނުވުން.

6.1.3 އެނެކްސް 3 (އަގުގެ ހުށަހަޅާ ކަރުދާސް)ގެ ޖުމްލަ އަގު އަދި މުއްދަތު ސާފުކޮށް އެނގޭގޮތަށް ނެތުން.

6.1.4 އެނެކްސް 4 (ބެލަން ހުށަހަޅާ ފަރާތުން ހުށަހަޅަންޖެހޭ ތަކެތި އަދި ޗެކްލިސްޓް) ގައި ބުނެފައިވާ ލިޔުންތަކުގެ ތެރެއިން ލިޔުމެއް ހުށަހަޅާފައި ނުވުން.

6.1.5 އަގު ހުށަހަޅާ ފޯމުތަކުގައި (އެނެކްސް 3 ގައިވާ އަގުގެ ހުށަހަޅާ ކަރުދާސް އަދި ހުށަހަޅާ އެސްޓިމޭޓް، ކޮޕީ ސްކޭން، ބީ.އޯ.ކިއު ނުވަތަ އަސްލާސް ރިޕޯޓް) ބެލަން ވެރިޔާގެ ސޮއިއާއި ކުންފުނީގެ ތައްގަނޑު ނެތުން.

6.1.6 ބެލުމުގެ މުއްދަތު ހަމަވާ ތާރީޚަށް، ބެލަން ހުޅުވާ ތާރީޚުން ފެށިގެން 120 ދުވަސްތެރޭގައި ނުވުން.

6.1.7 އެފަރާތަކުން ހުށަހަޅާ ޕްރޮޖެކްޓްތަކުގެ ބިޑްސެކިއުރިޓީ/ބޭންކްގެރެންޓީ ސެކިއުރިޓީ ކޮޕީ ސާފުކޮށް ލިޔުން އަދި ޗެކް ހިމަނާފައިނުވުން.

7. ބެލަމާއެކު ހުށަހަޅަންޖެހޭ ތަކެތި

7.1 އެނެކްސް 4 (ބެލަން ހުށަހަޅާ ފަރާތުން ހުށަހަޅަންޖެހޭ ތަކެތި އަދި ޗެކްލިސްޓް) ގައި ބުނެފައިވާ ލިޔުންތަކުގެ ތެރެއިން މި ބެލަމާއެކު ހުށަހަޅަން ބުނެފައިވާ ލިޔުންތައް ހުށަހަޅަންވާނެއެވެ.

8 ތަޖުރިބާ ލިޔުން ހުށަހެޅުން

8.1 ތަޖުރިބާ ހުރި މިންވަރު ހާމަކުރުމުގެ ގޮތުން މަސައްކަތްކޮށްދީފައިވާ ތަންތަނުން ލިޔުން ހުށަހަޅާއިރު މި މާއްދާގައި ބަޔާންކޮށްފައިވާ ކަންކަން ފުރިހަމަވާން ޖެހޭނެއެވެ.

8.2.1 ވޯކް ޕްރޮފައިލް 4 އަހަރުގެ ތެރޭގައި ކޮށްފައިވާ މަސައްކަތްތަކުގެ ލިޔުމެއްކަމުގައިވުން.

8.2.2 މި އިދާރާއާ ގުޅިގެން ކުރަންޖެހޭ މަސައްކަތާއި ގުޅުންހުރި ލިޔުމެއްކަމުގައިވުން.

8.2.3 މަސައްކަތް ފުރިހަމަކުރުމުން ދޫކުރާ ލިޔުމެއްކަމުގައިވުން.

8.2.4 މަސައްކަތް ނިންމަންޖެހޭ މުއްދަތަށް، މަސައްކަތް ނިންމާފައިވާކަން އެނގެން ލިޔުމެއްކަމުގައިވުން.

8.2.5 މިގޮތުން ހުށަހަޅާ ލިޔުންތަކުގައި މަސައްކަތުގެ ތަފްސީލު، ޖުމްލަ އަގު، މުއްދަތު، މަސައްކަތް ހަވާލުކުރެވުނު ތާރީޚު، ނިންމަންޖެހޭ ތާރީޚު އަދި މަސައްކަތް ނިންމި ތާރީޚު އެނގެން އޮންނަންވާނެއެވެ.

8.2.6 އަދި ތަޖުރިބާ ހުރި މިންވަރު ހާމަ ކުރުމުގެ ލިޔުން ހުށަހަޅާނަމަ، ހުށަހަޅާ ލިޔުމުގެ އަދަދު އެނެކްސް 5 (ބެލަން ހުށަހަޅާ ފަރާތުން ކޮށްފައިވާ ގުޅުންހުރި މަސައްކަތްތަކުގެ ތަފްސީލް)ގައި ހިމަނަންވާނެއެވެ.

9\. ބީލަންތައް އިވެލުއޭޓް ކުރުމާއި ބީލަމުގައި ބައިވެރިވި ބީލަންވެރިންނަށް މުއްދަތު ދިނުން

9.1 އިވެލުއޭޝަންގެ ކޮމިޓީއަށް ބީލަންތައް ބަލައިގަނެ، ބީލަންތައް ވަޒަންކޮށް، ބީލަން ހުށަހެޅުމަށް ދެވިފައިވާ މުއްދަތުތަކާއި ޝަރުތުތަކާއި ބީލަން އިވެލުއޭޓް ކުރުމަށް ބޭނުންކުރާނެ ކްރައިޓީރިއާ މިންގަނޑަށް ބަލައިގެން ފުރިހަމަކޮށްފައިވާ ބީލަމުގެ ބައިވެރިކަން ވާރކްސް ދެވޭނެއެވެ.

9.2 ބީލަން ހަވާލުކުރާނީ ފަރާތެއް ކަނޑައަޅާއިރު ޝަރުތު ފުރިހަމަވާ ފަރާތްތަކުގެ ތެރެއިން އެންމެ މަތިން މާކްސް ލިބޭ ފަރާތަކަށެވެ.

9.3 ބީލަމުގައި ބައިވެރިވި ބީލަންވެރިންނަށް މާލިއްޔަތުގެ ގަވާއިދުގެ 10.47ގައި ބަޔާންކޮށްފައިވާ ގޮތުގެމަތިން މުއްދަތު ހަމަކުރެވޭނެއެވެ.

10\. އެއްބަސްވުމުގެ އާންމު މާއްދާތައް އަދި ޚާއްޞަ މާއްދާތައް

10.1 **އެއްބަސްވުމުގެ ދަރަނި ގަނޑު ތަކެތީގެ ނުވަތަ ކުރަންޖެހޭ މަސައްކަތާއި ޢަދަދާއި ހިދުމަތް:**

އެއްބަސްވުމުގެ ދަރަނި ގަނޑު ތަކެތީގެ ނުވަތަ ކުރަންޖެހޭ މަސައްކަތާއި ޢަދަދާއި ހިދުމަތުގެ ތަފްސީލު މި ޕްރޮޖެކްޓްގެ ދަރަނި ހަމަ އެއްބަސްވުމުގައި ބަޔާންކޮށްފައިވާނެއެވެ.

10.2 **ލިޔެކިޔުން ބަދަލުކުރުން**

10.2.1 އެއްބަސްވުމުގައި ޝާމިލުވާ ފަރާތްތަކުން މިއެއްބަސްވުމާއި ގުޅިގެން އެއްފަރާތުން އަނެއްފަރާތަށް އަންގަންޖެހޭ އެންގުމަކީ އެންގުންތައް އާންމު ގޮތެއްގައި އަންގާނީ ދިވެހިބަހުން، ލިޔުމުންނެވެ.

10.2.2 އެއްފަރާތުން އަނެއްފަރާތަށް ފޮނުވާލިޔުން ރައްދުކުރާނީ މި ކޮމިޝަނުގެ ރަސްމީ ސަރވަރ ނުވަތަ tender@elections.gov.mv އީމެއިލް އެޑްރެހަށެވެ.

10.3 **އެއްބަސްވުމުގެ މުއްދަތު**

10.3.1 އެއްބަސްވުމުގެ ދަރަނި ގަނޑު ތަކެތީ، ކުރަންޖެހޭ މަސައްކަތާއި، ޢަދަދާއި ހިދުމަތް ފޯރުކޮށްދޭނޭ މުއްދަތަކީ މި ޕްރޮޖެކްޓްގައި ގެލެން ހަމަ އެއްބަސްވުމުގައި ބަޔާންކޮށްފައިވާ މުއްދަތެވެ.

10.3.2 މަސައްކަތް ހަވާލުކުރި ފަރާތުގެ އިހުމާލުން ހިނގާކަމެއް ނުވަތަ ލަސްވާ ލަސްވުމެއް މުއްދަތުގެ ތެރޭގައި ނުގެންނާނެއެވެ.

10.3.3 މަސައްކަތް ހަވާލުވި ފަރާތުގެ ބާރުން ބޭރުގެ ކަމެއް ނުވަތަ ޤުދުރަތީ ހާދިސާއެއް/ކާރިސާއެއް ނުވަތަ ގުނިފުރާނައިގެ ކަމެއް ކުރިމަތިވެގެން ދަތިވާ މުއްދަތު އިތުރުކުރަންޖެހިއްޖެ އެކަމެއް ދިމާވިކަން އެގޮތަށް ރަސްމީ ނުވަތަ ކަމާގުޅޭ ފަރާތްތަކުގެ ލިޔުންތަކާއެކު މަސައްކަތް ނިންމަންޖެހޭ މުއްދަތު ހަމަވުމުގެ ކުރިން މި އިދާރާއަށް ހުށަހަޅަންވާނެއެވެ.

10.3.4 މަސައްކަތް ނިމުމުގެ ކުރީ ދުވަސްތައް މުއްދަތަށް އިތުރުކުރެވޭނީ އެކަމެއް ބަލައި ދައުލަތުގެ މާލިއްޔަތުގެ ގަވާއިދުގެ 10.49ގައި ބަޔާން ކޮށްފައިވާ ގޮތުގެމަތިން ބޭނޭ ކޮމިޓީއަށް ހުށަހަޅައިގެންނެވެ.

10. ގުޅުވެދޭ ފަރާތް ފޯނު ނަންބަރު ލިޔުން

10.4 **ގުޅުވެދޭ ފަރާތް ނިންމާ ފަރާތް، ޕާޓީ ފޯނު ނަންބަރު ލިޔުން**

10.4.1 ގުޅުވެދޭ ފަރާތް ހަމަ ކަންތައް ކުރަމުންދާ ފަރާތެއް ކަމަށް 10.65 ގައި ފާހަގަ ކުރެވިފައިވާ ފޯނު ނަންބަރު ލިޔުން ދިނުން.

10.4.2 ގުޅުވެދޭ ފަރާތް ކަންތައް ކުރަމުންދާ ފަރާތާ ވަކި ކުރެވިދާނެ ގޮތަށް ބަލައިގަންނަ ފަރާތެއް ("ނިންމާ ފަރާތް") ހުށަހެޅުން ފުރިހަމަ ކުރުމަށް ގުޅުވެދޭ ފަރާތް ކަންތައް ކުރަމުންދާ ފަރާތާ ގުޅުވައި ދިނުން.

10.5 **ގުޅުވެދޭ ފަރާތުގެ ލިންގ:** ގުޅުވެދޭ ފަރާތް ބަލައިގަންނަ ފަރާތާ ގުޅުވައި ދިނުމަށް ފަރާތުން ދެކެ ގުޅުވެދޭ ފަރާތް ފިރިހެންކަން ނުވަތަ ފަރާތުން ދެކެ ގުޅުވެދޭ ފަރާތް ތަކެއް ކަމަށް ބަލައިގަންނަ ފަރާތާ ގުޅުވައި ދިނުން.

10.6 **ގުޅުވެދޭ ކަންތައް:** ގުޅުވެދޭ ފަރާތް ސާވިސް ޕްރޮވައިޑަރ ކުންފުނިއެއް ކަމަށް ބަލައިގަންނަ ފަރާތާ ގުޅުވައި ދިނުމުގައި ކުންފުނީގެ ވެބްސައިޓް ނުވަތަ ފޭސްބުކް ޕޭޖު ފަދަ ކުންފުނީގެ ސޯޝަލް ވެބްސައިޓް ބެލެހެއްޓުމަށް ކުންފުނީގެ ފަރާތުން ދީފައިވާ ފަރާތާ ގުޅުވައި ދިނުން. ގުޅުވެދޭ ފަރާތް ކުންފުނީގެ ވެބްސައިޓް ބެލެހެއްޓުމަށް ކުންފުނީގެ ފަރާތުން ދީފައިވާ ފަރާތާ ގުޅުވައި ދިނުން.

10.7 **ލޮގިން ތަފްޞީލު ފޮނުވުން:** ފޯނު ނަންބަރަށް ލިންކެއް ފޮނުވުމުގެ ކުރިން ލޮގިން ތަފްޞީލު ފޮނުވުން، ލޮގިން ތަފްޞީލު ފޮނުވުމަށް ކުރިން ލޮގިން ތަފްޞީލު ފޮނުވުމަށް ކުންފުނީގެ ފަރާތާ ގުޅުވައި ދިނުން.

10.8 **ގުޅުވެދޭ ފަރާތުގެ ތަފާތު:** ގުޅުވެދޭ ފަރާތް ކުންފުނީގެ ތަފާތު ފަރާތެއް ކަމަށް ބަލައިގަންނަ ފަރާތާ ގުޅުވައި ދިނުން.

10.9 **ގުޅުވެދޭ ފަރާތުގެ ދާއިރާ:** ގުޅުވެދޭ ފަރާތް ފަރާތުގެ ދާއިރާ، ތަކެއް ބަލައިގަންނަ ފަރާތާ ގުޅުވައި ދިނުން.

10.11 **ފުރަތަމަ ގުޅުވުން**

10.11.1 ގުޅުވެދޭ ފަރާތާ ފުރަތަމަ ފަހަރަށް ގުޅުވައި ދިނުމުގައި ބަލައިގަންނަ ކަންތައް ކުރަމުންދާ ފަރާތާ ގުޅުވައި ދިނުން، ފަރާތުގެ ނަން ބަލައިގަންނަ ފަރާތާ ގުޅުވައި ދިނުން.

10.11.2 ގުޅުވެދޭ ފަރާތް ކަންތައް ކުރަމުންދާ ފަރާތާ ގުޅުވައި ދިނުމުގައި ބަލައިގަންނަ ފަރާތާ ގުޅުވައި ދިނުން، ފަރާތުގެ ނަން ބަލައިގަންނަ ފަރާތާ ގުޅުވައި ދިނުން.

Elections Commission
PA Complex, 5th Floor, Malé
20307, Republic of Maldives
T (960) 332 2241
F (960) 332 3997
www.elections.gov.mv

·10	ގުޅުވެދޭ ތަކެތީގެ ބަދަލުގައި ދެއްކޭ ފައިސާ	10·12 **ގުޅުވެދޭ ތަކެތީގެ ބަދަލުގައި ދެއްކޭ ފައިސާ** ކަނޑައެޅިފައިވާ ގޮތަށް ގުޅުވެދޭ ތަކެތީގެ ބަދަލުގައި ދެއްކޭ ފައިސާ ދޫކުރުމުގެ ގޮތުގައި ދެއްކޭ ފައިސާ 10·70ގައި ބަޔާންކޮށްފައިވާ ގޮތަށް ދެއްކުމަށް ގަބޫލުކުރަންވާނެ.
·11	ފޮތުން ތައްޔާރުކުރުން	11·1 ފޮތުން ތައްޔާރުކުރުމަށް ބޭނުންކުރާ ކޮންޕިއުޓަރ ސޮފްޓްވެއަރ ތަކުގައި ވާންޖެހޭ ގޮތުގެ ތަފްޞީލު ކަނޑައެޅިފައިވާނެ.

ދަނޑި 80 ގެ ގޮތުގައި

ގުޅުވެދޭ ދަނޑި ހިފާ ގޮތުގައި ދެއްކޭ ފައިސާ ދަނޑި ގެ ގޮތުގައި ބަލައިގަނެ ދެއްކުމަށް ގަބޫލުކުރެވެއެވެ. ގުޅުވެދޭ ތަކެތި ގަނެ ދެއްކުމަށް ކުރިން ދެއްކުމަށް ބާއްވާ ކޮންޓްރެކްޓުގައި ބަޔާންކުރާ ގޮތަށް ދެއްކުމަށް ގަބޫލުކުރެވެއެވެ.

$$\text{ދެއްކުމަށް ބާއްވާ ފައިސާ} = \text{ގުޅުވެދޭ ތަކެތި ގަނެ ދެއްކުމަށް ބާއްވާ ދަނޑި} \times 80$$

ކަނޑައެޅިފައިވާ ގޮތުގެ ގޮތުގައި 20 ގެ ގޮތުގައި

ކަނޑައެޅިފައިވާ ގޮތުގެ ފަރާތްތަކާ ދެކޮޅަށް 8·1 ގައިވާ ގޮތަށް ހިންގާ ކޮންޓްރެކްޓް ގައި ބަލައިގަނެ ހިންގާ ކޮންޓްރެކްޓުގެ ތަފްޞީލު ގުޅުވެދޭ ތަކެތި ގަނެ ދެއްކުމަށް ބާއްވާ ފައިސާ ދަނޑި ގެ ގޮތުގައި ބަލައިގަނެ ދެއްކުމަށް ގަބޫލުކުރެވެއެވެ. ގުޅުވެދޭ ތަކެތި ގަނެ ދެއްކުމަށް ކުރިން ދެއްކުމަށް ބާއްވާ ކޮންޓްރެކްޓުގައި ބަޔާންކުރާ ގޮތަށް ދެއްކުމަށް ގަބޫލުކުރެވެއެވެ.

$$\text{ދެއްކުމަށް ބާއްވާ ފައިސާ} = \text{ކަނޑައެޅިފައިވާ ގޮތުގެ ގޮތުގައި} \times 20$$

އެނެކްސް-1 (މައުލޫމާތު ކަރުދާސް)

1. Introduction

The Elections Commission of Maldives (herein referred as ECM) is seeking qualified vendors to submit proposals for the supply and delivery of an advanced endpoint protection solution. The objective of this procurement is to enhance our cybersecurity posture by implementing robust, scalable, and centrally managed protection for all endpoint devices across our organization.

The successful bidder will be expected to provide a solution that offers comprehensive threat prevention, detection, and response capabilities, along with timely updates, technical support, and clear deployment guidance. This initiative aims to safeguard our network, systems, and data against evolving cyber threats while ensuring compliance with applicable security standards.

2. Technical & Functional Specifications

2.1. General Requirements

- 2.1.1 The Endpoint Security Solution setup must have the capability to scale the number of endpoints, which may be implemented in phased manner.
- 2.1.2 The proposed solution should support either Saas based platform or on-premises deployment
- 2.1.3 In case of on-prem solution bidder will provide requisites hosting hardware & all necessary software within the quoted price. Only cost of proxy servers will be quoted separately.
- 2.1.4 The bidder must ensure that hardware/software required at the central console can scale to onboard additional endpoints at any time.
- 2.1.5 Solutions features must be fully compatible over IPv4/IPv6 network such as hardware, software and application software etc.
- 2.1.6 Solution should have management infrastructure, operational monitoring, upgrades, reporting, notifications & 24x7 support.
- 2.1.7 The quoted solution must be part of MITRE ATTACK evaluations or any other equivalent evaluation programs during last 3 years.
- 2.1.8 The proposed solution shall include licensing for a minimum of 335 endpoints, covering all required features and functionalities.
- 2.1.9 The proposed licensing shall be valid for a period of one (1) year from the date of activation.

2.2. Management Console

- 2.2.1 The solution should provide a unified web-based console for all functionalities and should allow administrators to access the management interface to any authorized user, without installing additional software
- 2.2.2 The solution should support multi-site configuration and multiple tenants within same organization.

2.2.3 The solution should provide the flexibility to have individual rules/policies for every group. The solution should also support policy inheritance from Account to Site to Group with the ability to break inheritance if required.

2.2.4 The proposed solution must have the option to create role-based access/view(s) of the management console.

2.2.5 The solution should provide API access to all management capabilities and access to data. API should be well documented and available without any additional cost and application and hardware. The solution should have ability to quickly run APIs on the console data set without any limitations.

2.2.6 Solutions must provide multi-factor authentication and single sign-on solutions for the management console and sensitive functions such as remote shell.

2.2.7 Solution must provide non-repudiable Centralized auditing and logging of activity through the management console. Management activity must be logged and audited with the ability to send logs to an external source without restrictions.

2.2.8 The centralized management console should support features such as below:

- 2.2.8.1 File hash Information collection
- 2.2.8.2 Termination of the service
- 2.2.8.3 Download of binary
- 2.2.8.4 Addition of hash value to block list
- 2.2.8.5 Delete the file
- 2.2.8.6 Send the hash to get the verdict (Threat Intelligence integration)
- 2.2.8.7 Execute a python script
- 2.2.8.8 Execute a PowerShell script

2.3. Endpoint Agent Capabilities

2.3.1 Endpoint Agent must provide Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) capabilities available in a single agent without requiring multiple software packages to be installed. Besides this, all the other security features of the solution, e.g. Host Firewall, threat intel, Device Control, real-time analysis & threat hunting must be available via a single agent.

2.3.2 Endpoint Agent must provide strong anti-tamper capabilities, to ensure that an end user cannot remove, disable or modify the product in any way.

2.3.3 Endpoint Agent must support ability to on-demand scans (from console and/or endpoint) to look for malware or ensure a threat has been remediated.

2.3.4 The proposed solution must have capability to schedule agent upgrades from the management console.

2.3.5 Endpoint Agent must have ability to temporarily disable agent via the management console for temporary troubleshooting or testing.

2.3.6 Licenses should not restrict features of the solution, in case of license count exceeding in emergent/unintended circumstances.

2.3.7 Solution should have feature of automatically decommissioning old agents if they haven't communicated to the management server for a configurable period. As and when connection to the system is established the agent must be auto populated in the console.

2.3.8 Endpoint Agent must be lightweight with minimal system resource utilization for standard system usage (<3% CPU, <350 MB of memory).

2.3.9 Agents must support remote uninstallation from the management console.

2.3.10 Agent must support display of customized alert messages on managed endpoints.

2.3.11 Deployed agents must be able to communicate with the central management server via a web proxy.

2.3.12 The proposed solution shall be able to provide the visualization flow of the chain of events. It must include processes in the chain that happen before the malicious process

2.3.13 The proposed solution shall support the collection of forensic data using the same EDR agent without making any changes in the system (Endpoint Machine) configuration.

2.4. Operating System Support

2.4.1 Solution must support all versions of Windows Operating Systems starting from windows 7 SP1 for endpoints and Windows server 2008 onwards servers.

2.4.2 Solution should support all the latest virtual environments.

2.4.3 Agent supports all MacOS's starting from macOS Mojave (10.14).

2.4.4 Solution should support all the latest Linux environments Amazon, CentOS (6.4+ and above), Debian (8 and above), Fedora, Oracle, Red Hat Enterprise Linux (6.4 - 6.10 and above), SUSE Linux Enterprise Server (12.X and above) Ubuntu (18.04, 16.04, 14.04, and above with LTS)

2.4.5 Solution must support all Windows OS for a minimum period of 12 months after the OS version is end of sale/life. Similarly, Solution must support all MacOS for a minimum period of 36 months after the OS version is end of sale/life

2.4.6 Solution should support all the new OS Updates/Versions within 60 days of release.

2.4.7 Solution must support Windows agent running in kernel space to ensure highest level of anti-tamper.

2.4.8 Mac agent should support Kextless architecture.

2.4.9 Linux agents must run solely in user space to avoid kernel panics and tainted kernels that invalidate support.

2.4.10 The proposed solution should provide protection against exploits including MacOS, Windows, Linux (Ubuntu & Centos Flavors) and processes

2.4.11 The proposed solution should provide context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. The solution must have features for Custom detection, intelligence, and controls.

2.4.12 EDR Solution must provide prevention across all major Operating Systems – Windows, MacOS and Linux.

2.4.13 EDR Solution must have capability to protect the system against known and unknown malwares.

2.4.14 EDR solution should ensure that files are checked for any infection on write and execute operations.

2.4.15 The solution should be effective against sophisticated attacks by analyzing Behaviors on an endpoint.

2.4.16 The solution should have mechanism to protect the endpoint against malware, even when the system is not connected to the network. The agent needs to be fully autonomous meaning it does not need not to have any dependency on Management Server or Cloud or any resources external from the Agent to detect and respond appropriately to sophisticated threats (Zero Day, File-less, Ram-based, Zero Day exploits, Ransomware, Miners, Lateral movement, Reconnaissance attacks , APT) in real time as the threats are detected.

2.4.17 EDR solution should leverage Artificial Intelligence or Machine Learning to analyze files pre-execution as well as analyze behaviors while a file is running.

2.4.18 The solution should have capability to detect dormant threats as well.

2.4.19 The EDR solution should support equivalent protection capabilities across Windows, Mac and Linux.

2.4.20 The solution should protect endpoints from malicious documents and scripts.

2.4.21 The solution should monitor and protect the system from lateral movements & insider threats.

2.4.22 The EDR solution should monitor and protect from exploits and file-less attacks.

2.4.23 The EDR solution should identify and block potentially unwanted programs on MAC based systems.

2.4.24 The solution should provide flexibility to safely download malicious or convicted files from the management console.

2.4.25 Threat alerts should be correlated together automatically across enterprise if related to the same attack.

2.4.26 The solution must identify data exfiltration via legitimate protocols (DNS tunneling, ICMP tunneling).

2.4.27 The solution must identify and block credential theft attempts occurring in memory. (Credential dump, brute force, Denial of Service (DoS) & SQL Injection) or network traffic (ARP spoofing, DNS Responder).

2.4.28 Solution must have multi-method prevention techniques which include signature, signatureless, file less, memory based, shell code and threats/exploit

2.4.29 Solution should have mechanisms to manage encryption like BitLocker or filevault

2.4.30 Solution should provide casualty view / process tree, graph for each telemetry received from agent, it must not depend on any triggering mechanism like alert or condition.

2.4.31 Solution should detect and notify in case any anomaly in case any change in user behavior.

2.4.32 Solution should be able to detect any session hijacking, Active directory & Single sign-on attack.

2.4.33 Solution should be able to detect and notify for any rare process, task execution along with associated identity to identify and mitigate suspicious activity.

2.4.34 Solution should have similar level of exploit protection across all operating systems e.g. Windows, Linux, MacOS.

2.4.35 The proposed solution shall be able to provide real-time prevention against exploits of application vulnerabilities by blocking through core exploit techniques not limited to Software Logic Flaws, Memory Corruptions, code execution, DLL Hijacking, etc.

2.4.36 The Proposed solution should support backward and forward matching of IOCs and Custom Behavioral Indicators.

2.4.37 The proposed solution should perform multi-level search across endpoints using rich-search criteria And User-defined criteria like Username, File - Name, File - Hash (MD5, SHA1 and SHA2), IP address, Hostname, Registry Key, Registry Value Name & Registry Value Data

2.4.38 The proposed solution should be able to create multi-stage detailed kill-chain for performing the root cause analysis of an incident. Kill chain also provide reputation of the files from the global threat intelligence as well.

2.4.39 The proposed solution to provide the advanced response capabilities as mentioned below

2.4.39.1 Kill Processes, Isolate Devices, Block Processes

2.4.40 Solution should support a full remote shell for all OS (Mac, Windows, Linux) and not limit or restrict to set of commands.

2.4.41 Solution should track all remote shell commands and logged during a remote shell session.

2.4.42 Solutions should alert both suspicious and malicious threat behavior.
2.4.43 Solution should have ability to kill and quarantine an offending process.
2.4.44 Solution should be able to un-quarantine a file from the management interface or API.
2.4.45 Solution should have ability to remediate all operating system changes and perform corrective action. Tool should also be able to undo any system level changes related to the attack (Registry edits, configuration changes etc.)
2.4.46 Solution should have options to reverse destructive data events including but not limited to ransomware. The tool should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state.
2.4.47 Detect Cloud-Based Attacks Such as Exploits, Ransomware, Cryptojacking, And Web Shells.
2.4.48 The solution should provide the option to network quarantine a device and provide flexibility to configure the select allow list during quarantine
2.4.49 Threat response capabilities offered by the solution should be automated.
2.4.50 Solution should provide a mechanism to take remedial actions on multiple systems at once.
2.4.51 Solution should have options to add notes or set the status of an issue or event (i.e. resolved, in progress, unresolved)
2.4.52 The solution provided should support static, dynamic, bare metal & recursive analysis etc.
2.4.53 Tool should provide Ability to support policy inheritance across an account, site or group of devices
2.4.54 Tool should have the option to provide dynamic policy assignment based on device attributes
2.4.55 Devices should be installed and placed directly into a specific device group at time of installation
2.4.56 The policy context should provide the option to turn ON or OFF unique engines or by Type of engine (Pre-Execution and Run-Time Engines).
2.4.57 The product should have predefined list of known or recommended exclusions
2.4.58 Tool should provide the option for the administrators to make policy exclusions of the console at multiple levels. (Account, Site, Group)
2.4.59 Provide option for exclusions be deployed in a highly granular way to make the smallest exception possible while still supporting interoperability.
2.4.60 Provide option for Administrators to configure exclusions to independently suppress alerts related to file-based machine learning and/or behavioral engines

2.4.61 Exclusions to be configured by the administrator to handle interoperability issues down to specific paths or single executables by reducing monitoring of parent processes and/or parent processes and all their spawned child processes

2.4.62 Provide options for exclusions be made by administrators of the console for the following parameters

2.4.62.1 Hash and Path

2.4.62.2 Certificate or Signer ID

2.4.62.3 File Type

2.5. Device Control & Application Visibility

2.5.1 Tool to have the capability to control external USB media and fine tune Block policy to allow only 'Read only' access to the USB media including mobile.

2.5.2 Tools should have the capability to control external Bluetooth devices including mobile

2.5.3 The proposed solution should have granular device control capability which can be applied to a Class, Serial Number Product ID or Type of Device.

2.5.4 Device control capabilities should be available on Mac and Windows

2.5.5 The proposed solution must provide a software/application inventory for the environment and identify unpatched 3rd party software apps that may have vulnerabilities

2.5.6 Device control capabilities should be available on Mac and Windows

2.5.7 The proposed solution must provide a software/application inventory for the environment and identify unpatched 3rd party software apps that may have vulnerabilities

2.5.8 Device control capabilities should be available on Mac and Windows

2.5.9 The proposed solution must provide a software/application inventory for the environment and identify unpatched 3rd party software apps that may have vulnerabilities

2.5.10 The proposed solution should report all known vulnerabilities in programs installed on an endpoint, along with export options.

2.5.11 The solution must have the capability to Run scripts on multiple endpoints based on groups/individual to automatically collect forensic artifacts and expedite triage and response to reduce MTTR with immediate response actions to contain and terminate threats.

2.5.12 Software Tools Installation and uninstallation on multiple endpoints through script execution feature through management console.

2.5.13 Precooked script from OEM to collect data and take remedial action through management console on endpoints.

2.5.14 Host Based Firewall Control

2.5.15 The solution should provide Firewall Control for Windows, MAC & Linux. it must not be limited to Windows only. The firewall control policy should provide context unique to each group of Endpoints. Firewall and should support FQDN's, IP, CIDR, Range.

2.5.16 The proposed solution should have Firewall rules be built to apply to a specific group of devices (leveraging tagging or policy groups)

2.5.17 Firewall rules should be location aware to apply different policies when on or off network

2.6. Device & Network Discovery

2.6.1 Solution must have capability to implement policies for rogue devices to reduce the potential attack surface, and Actions could include isolate (prevent communication from rogue devices) or installing an agent.

2.6.2 The proposed solution must have the capability to manage the Live global asset inventory, Advanced ML device fingerprinting with flexible active + passive scanning and isolating suspicious and malicious devices.

2.6.3 The solution should automatically discover IoT devices in a network without the need to deploy sensors, sniffers or other hardware.

2.6.4 The solution should provide flexibility to ensure discovery is only occurring on desired networks

2.6.5 The solution should have the ability to actively scan for, and fingerprint unmanaged and IoT devices. The solution should provide the means to search for devices based on device class (Video, Mobile, Printer, Infrastructure, Server, Workstation, IPPhone, Storage, Virtual Machine)

2.7. Integrations

2.7.1 The solution must have capability to Integrate with Active Directory

2.7.2 The solution should have native integrations with SIEM solutions such as Splunk & Qradar etc.

2.7.3 The product should stream EDR data in real-time to own internal data lake

2.7.4 EDR solution should natively send event logs via Syslog. The solution must support the following syslog formats: CEF, CEF2, RFC-5424, STIX and IOC. It should support SSL and X.509 certificates for syslog transport encryption and authentication.

2.7.5 The solution must have capability to API integration

2.8. Dashboards & Reporting

2.8.1 The proposed solution must identify rogue devices' discovery capability to reduce the potential attack surface, with Network exclusion capability

2.8.2 The proposed solution has option to export data into 3rd party reporting tools.

2.8.3 The proposed solution must have inbuilt and customizable dashboards and reporting capability per Site /Group and user.

2.8.4 The Solution should have capability to report all known vulnerabilities in programs installed on an endpoint, along with export option.

2.8.5 The dashboards should be customized per user

2.8.6 Solution should support Incident merge with another similar incident to reduce the analyst workload in managing operations.

3. Warranty, Support & Maintenance

3.1. The bidder should provide a One Year Warranty for the respective requirements included in the proposed solution.

3.2. A comprehensive SLA must be provided with the proposal for one year.

3.3. The proposed solution should offer an option to have a technical account manager or higher level of support, please outline the offering & SLA's.

3.4. The proposed solution should offer services to assist with the deployment and configuration of the solution.

3.5. The proposed solution must provide Customer receive 24x7x365 support coverage, follow-the-sun support for Severity-1 and Severity -2

3.6. Vendor should have optional web based/on-demand training as well as live/in-person training, please provide available training courses.

3.7. The bidder must Provide security-focused technical expertise and support, Project planning/management and documentation

4. Delivery and Installation Schedule

4.1. The vendor shall deliver hardware, install the software and integrate with existing infrastructure within 1 weeks from the date the project is awarded.

4.2. After completion of installation the bidder should obtain sign-off on the Installation-cum-Acceptance certificate from the ECM official. ECM will carry out acceptance of hardware/software as per acceptance test plan.

4.3. Installation will be treated as incomplete in one/all the following situations:

4.3.1 Non-delivery of any software or other components, accessories, documentation, drivers, media mentioned in the order.

4.3.2 Non-delivery of supporting documentation.

4.3.3 Delivery, but no installation of the components and/or software.

4.3.4 System operational, but unsatisfactory to ECM

5. Expectations from Bidders

5.1. As required by this RFP, the bid must be accurate, comprehensive, and in the format specified. As stated in points 1, 2, and 3, all suggested items must be accompanied by the relevant technical documents.

5.2. The vendor must provide at least 5 references where such systems have been installed on on-premises and are being maintained. (Reference from the client confirming the completion of the project).

5.3. The vendor must be an authorized incident response partner of the manufacturer of the proposed solution.

5.4. The vendor must provide a manufacturer authorization letter from the manufacturer of the proposed solution.

5.5. The proposed implementation team must include a minimum of 5 certified incident response engineers.

5.6. The technical Proposal should include solution design diagrams and specifications.

5.7. Proposed solutions and implementation must be delivered and carried out by the bidder. No component of the work can be allowed to be subcontracted.