بسم الله الرحمن الرحيم

ދާއިރާގެ ކުންފުނި ލިމިޓެޑް ތެރެ ހިންގާ ގަސް ކެނޑުން ހެދުމަށް

ޓެންޑަރ ގޮތް

ގަސް ކެނޑުން ހެދުމަށް ދާއިރާގެ ކުންފުނި ލިމިޓެޑް ތެރެ ހިންގާ ކަންތައްތަކުގެ ތަފްޞީލް	ގަސް ކެނޑުން ހެދުމަށް
PROC-2023-015	ގަސް ކެނޑުމުގެ ނަންބަރު
(IUL)164-PRO/1/2023/40	ހިއްސާކުރާ ނަންބަރު
05 ފެބްރުވަރީ 2023	ތާރީޚް

·1 ސެލްފީ ގަދައިގެ ލަވަ	
·1.1 ތަފާތު	ލިޔުންތެރިން ކަނޑައަޅާ ގޮތުގެ ތަފާތު ހުށަހަޅާ/ ހުއްދަ ދޫކުރާ ގޮތުގެ ތަފާތު.
·1.2 ލިބުންތެރި	
	ނަންބަރު (IUL)164-PRO/1/2023/40
	ލިބުންތެރި ތާރީޚް 05 ފެब्रުވަރީ 2023
	ކުރިއަރުވާ ގޮތުގެ ތަފާތު ތަކުގެ ތަފްޞީލު ތިރީގައި ބަލައި ބަލާ ގޮތަށް ފުރިހަމަ ކުރައްވާ
·1.3 ސެލްފީ ލަދުގަދަ	
	ގޮތް ކުރިއަރުވާ ގޮތުގެ ތަފާތު ތަކުގެ ތަފްޞީލު
	ބެލެނިވެރި NCIT ސެންޓަރު، 64 ސަތަ ކައިރި، ކާފޫގެ ހިސާބު
	ތާރީޚާ ގަޑި 17 ފެब्रުވަރީ 2023 ގައި 11:00 ގެ ކުރިން NCITގެ ތިބާގެ ބެލުން ބަލައިގަންނަވާ. ގެއިރުގައި ލަދުގަދަ ކުރާ ގޮތުގެ ތަފާތު ތަކުގެ ތަފްޞީލު ތިރީގައި ދެނެގަންނަވާ. ތާރީޚް (17 ފެब्रުވަރީ 2023) ހޯމަދުވަހު، ދިރާގު ތާރީޚާ ގަޑި 11:00 ގެ ކުރިން NCIT ގެ ތިބާގެ ބެލުން ބަލައިގަންނަވާ ގޮތުގެ ތަފާތު ތަކުގެ ތަފްޞީލު ތިރީގައި ދެނެގަންނަވާ.
·1.4 ސެލްފީ ލަދުގަދަ	
	ގޮތް ކުރިއަރުވާ ގޮތުގެ ތަފާތު ތަކުގެ ތަފްޞީލު ތިރީގައި ބަލައި ބަލާ ގޮތަށް ފުރިހަމަ ކުރައްވާ
	ބެލެނިވެރި NCIT ސެންޓަރު، 64 ސަތަ ކައިރި، ކާފޫގެ ހިސާބު
	ތާރީޚާ ގަޑި 17 ފެब्रުވަރީ 2023 ގައި 11:10 ގަދަ، ލިބުންތެރިން ތަންފީޒު ކުރާ ގޮތުގެ ތަފާތު ތަކުގެ ތަފްޞީލު ތިރީގައި ދެނެގަންނަވާ ތަކެއް ތިބެ ސެލްފީ ލަދުގަދަ ކުރާ ގޮތުގެ ތަފާތު ތަކުގެ ތަފްޞީލު ތިރީގައި ދެނެގަންނަވާ. ތާރީޚް (17 ފެब्रुވަރީ 2023) ހޯމަދުވަހު، ދިރާގު ތާރީޚާ ގަޑި 11:10 ގަދަ، ލިބުންތެރިން ތަންފީޒު ކުރާ ގޮތުގެ ތަފާތު ތަކުގެ ތަފްޞީލު ތިރީގައި ދެނެގަންނަވާ ތަކެއް ތިބެ ސެލްފީ ލަދުގަދަ ކުރާ ގޮތުގެ ތަފާތު ތަކުގެ ތަފްޞީލު ތިރީގައި ދެނެގަންނަވާ.

2.	ޕްރޮކިއުމަންޓް މަސައްކަތްތަކަށް ކުރިމަތިލާން ގޮތާއި އަމަލުކުރާނެ އުސޫލުތައް
2.1	މި ބީލަމަށް ބައިވެރިވާ ފަރާތަކީ / މަސައްކަތުގެ ތަފްސީލު މި ބީލަންފޮތުގެ ސެކްޝަން 3 ގައި ތަފްސީލުކޮށް ހިމެނިފައިވާނެއެވެ.
2.2	ބީލަމާއި ބެހޭގޮތުން އެއްވެސް ސުވާލެއްވާނަމަ، އީމެއިލް ކުރަނީ 2023 އޮކްޓޫބަރު 09 އާދިއްތަ ދުވަހު 11:00 ގެ ކުރިން tender@ncit.gov.mv އަށެވެ. އަދި އިސްތިފްސާރުތަކުން ސުވާލުގެ ހަވާލުތަކުގެ ކުރިން ހުށަހެޅޭ ސުވާލުތަކުގެ ޖަވާބުތައް މުއައްސަސާގެ ވެބްސައިޓް www.ncit.gov.mv ގައި 2023 އޮކްޓޫބަރު 12 ވާ ބުދަ ދުވަހުގެ 13:00 ގައި ޝާއިޢު ކުރެވޭނެއެވެ. މި ބީލަމަށް ހުށަހަޅާ ސުވާލު މުއައްސަސާއަށް އަންގާނީ ރިސާލާ ހުށަހަޅުއްވާ ފަރާތް ތަކުގެ ތެރެއިން އުފެދިފައިވާ ޒާތީކޮށްފިނަ ބީލަން ފޮރމް ނުވަތަ ބީލަންފޯރމްގެ ބަދަލުގައި އެފަރާތްތަކުން ކަނޑައަޅާ ފަރާތްތަކުގެ ޒާތީކުރެވޭނެއެވެ.
2.3	ބީލަން ހުށަހަޅާނީ ފަރާތްތަކުން (ކޮލިފިކޭޝަން ކްރައިޓީރިއާ) (ހ) ދަފްތަރުކޮށްފައިވާ ރަޖިސްޓްރޭޝަންކުރައްވާ ދަފްތަރު ވިޔަފާރިއަށްކަމުގައިވުން. (ށ) މާލީގޮތުން އިންތިޒާމު ރަނގަޅު އެކްރެޑިޓޭޝަން ރަޖިސްޓްރީކުރައްވާ ފަރާތަކަށްވުން.
2.4	ބީލަން ހުށަހަޅުއްވަންޖެހޭނީ، ވިޔަފާރީގެ ފަރާތުން އިދާރާއަށް ހާޒިރުވާ ފަރާތަކީ ބީލަމާއި ގުޅޭ އެންމެހައި ލިޔެކިޔުންތައްގައި ސޮއިކުރުމުގެ، ބީލަން ހުށަހަޅާ ފަރާތުގެ ހައްދު ނުވަތަ ފޮތަށް އޮތް އެޖެންޓް ލިޔުމެއްގެ ފަރާތުންކަމުގައި ބެލެވޭނެއެވެ.
2.5	ކޮލިފިކޭޝަން ކްރައިޓީރިއާގައި ހިމެނޭފައިވާ ކަންތައްތަށް ފުރިހަމަ ނުވާ ބީލަންތައް ބާތިލުވާނެއެވެ. އަދި މި ބީލަންތައް އިވެލުއޭޝަން މަރުހަލާއަކަށް ނުގެންދެވޭނެއެވެ.
2.6	ބީލަން ހުށަހެޅުމަށް ކަނޑައަޅާފައިވާ ސުންގަޑީ ހަމަވުމަށްފަހު ހުށަހަޅާ ބީލަންތައް ބަލައެއް ނުގަނެވޭނެއެވެ.
2.7	ބީލަންފޮރިން ހުށަހަޅާ ޕްރޮޕޯސަލް ހުށަހަޅަންވާނީ ތިރީގައި ބަޔާންކޮށްފައިވާ ގޮތަށެވެ. (ހ) ޕްރޮޕޯސަލްގެ ކޮޕީއެއް ސޮފްޓްކޮޕީއެއްގައި ނަންބަރު ޖަހާފައި ހުށަހަޅާ ވާނެއެވެ. (ށ) ޕްރޮޕޯސަލް ހުށަހަޅާނީ ބައިންޖެހޭ ކޮށްފައެވެ. (ނ) މި ފޮތުގެ ސެކްޝަން 4 ގައި ބަޔާންކުރާ ހުށަހަޅާ ތަކެތި ހަމަކުރަންވާނެއެވެ.
2.8	ބީލަން ހުށަހަޅާނީ ބަންދުކުރެވިފައިވާ ސިޓީއުރައެއްގައެވެ. އަދި ސިޓީއުރައިގެ ބޭރުގައި މި ތަންތަނާ މައުލޫމާތު ހިމަނަންވާނެއެވެ. (ހ) ބީލަމުގެ ނަން (ށ) އިއުލާން ނަންބަރު (ނ) ހުށަހަޅާ ފަރާތުގެ ނަން
2.9	ޕްރޮޕޯސަލްގައި ހިމެނޭ ކަންކަމާއި ގުޅޭގޮތުން އިވެލުއޭޝަން މަރުހަލާގައި އިދާރާއަށް ސާފުކުރުމަށް ބޭނުންވާ މައުލޫމާތު ލިޔުމުން ހުށަހަޅާ އިހުތިޔާރު އިދާރާއަށް ލިބިގެންވެއެވެ. އަދި އިދާރާއިން ބޭނުން ވެއްޖެނަމަ ލިޔުމުން ހުށަހަޅައިދިނުމަށް، ބީލަން ކޮށްފައިވާ ހުރިހާ އިހުތިޔާރު އިދާރާއަށް ލިބިގެންވެއެވެ.
2.10	ހުށަހަޅާ ބީލަމުގެ ބިޑް ވެލިޑިޓީ ޕީރިއަޑް ދުވަސްތަކުން މުއްދަތަކީ 90 (ނުވަދިހަ) ދުވަހެވެ.
2.11	މުއައްސަސާއަށް ހަވާލުކުރާން ފަރާތުން ހުށަހަޅާ ފޯރުކޮށްދޭ ތަކެތީގެ ކޮލިފިކޭޝަން ކްރައިޓީރިއާ އާއި އެއްގޮތަށް މާކުސް ދިނުމުން، އެންމެ މަތިން މާކުސް ލިބޭފަރާތަކަށެވެ.
2.12	މާލީ ޑޮކިއުމަންޓް ވަޒަންކުރާނީ ގޮތް މި ފޮތުގެ 6.3 ގައިވާ ގޮތުގައި ބަޔާންކޮށްފައިވާނެއެވެ.
2.13	ބީލަން ކާމިޔާބުވާ ފަރާތަކާއި އެކަން ރަސްމީކޮށް އަންގާނެއެވެ.
2.14	ބީލަން ކާމިޔާބުކުރި ފަރާތަށް ކޮންޓްރެކްޓް ހަވާލުކުރުމުގެ ކުރިން، ބީލަމުގައި ބައިވެރިވި ހުރިހާ ފަރާތްތަކަށް، އެބީލަން ކާމިޔާބުކުރި ކޮންފަރާތަކަށް ކަމާއި، ކާމިޔާބު ނުވާ ފަރާތްތަކަށް ކޮބައިކަން އަންގާނެއެވެ. އަދި ބީލަން

	ކާރިއްޔާ ދާއިރާގެ ތެރެއިން ގުޅުން ހުރިހާ ގޮތަކުން 5 (ފަސް) ދުވަހުގެ ތެދުވެރިކަމުގައި ހުންނަންވާނެ.
2.15·	ހަނގުރާމަ ދުއްތަކާ ގުޅުންހުރި ހަނގުރާމަ ކަންތައްތަކުގެ ތެދުވެރިކަމުގައި ވާނެ.
2.16·	ތެދުވެރިކަމުގެ ބާރުގެ ދަށުގައި ހިންގާ ފަރާތުން 6 ގަޑި ވަންދެން ހުއްޓާ.

3· ކުރިއަށްގެންދާ ހިދުމަތްތަކުގެ ބަދަލުގައި
3.1· ދެއްވާ ހިދުމަތަށް ތަކެއްޗާ ބެހޭގޮތުގައި ވަގުތީ ހިފެހެއްޓުން ވަގުތީ ހިފެހެއްޓުން
3.2· ތިމާވެއްޓާ ގުޅުންހުރި ކަންކަމުގައި ދަތިތަކެއް ދިމާވުމުން 24 ގަޑިއިރު، ކުރިއަރާ ގެންދާ ތަރައްޤީ ތަކެއް ކަމަށް ދެއްވާ ކަމަށް، ކަނޑައަޅާ ލިޔުންތައް
3.3· ފާސްކުރުން، ކުރިއަށް ގެންދާ ކަންކަމުގައި ބަދަލުތަކެއް ގެނައުން ހިންގާ ފަރާތުން ކަނޑައަޅާ ލިޔުންތައް
3.4· ތަކެއްގެ ގޮތުގައި ބަލައި ގެންދާ ކަންކަމުގައި ބަދަލުތަކެއް ގެނައުން ހިންގާ ފަރާތުން ދަތުރުގައި ދާ ފަރާތްތަކުގެ ތަކެތި ބަލަހައްޓަން ދެވޭ ގޮތް

ދަތުރުކުރާ ފަރާތުގެ ތަފްޞީލު

ދާއިރާގެ ގޮތުގައި ކުރަންވާ ތަކެއްޗާ ގުޅިގެން ސަލާހުކުރުމަށް ކަނޑައެޅިފައިވާ ކޮންސަލްޓަންޓުންނާ ގުޅިގެން ދަތުރުކުރާ ފަރާތުގެ ތަފްޞީލު ތިރީގައި ހިމެނޭ ފަދައިން ފުރިހަމަ ކުރަންވާނެ.

Scope of Services

1. Assisting in developing national strategies and legislations of cybersecurity; Ensuring the dissemination of best practices in the fight against existing and emerging cybercrimes.
2. Promoting accuracy and integrity of ICT data at the national, regional and continental levels and identifying gaps in evidence and suggesting priority research areas in the field of cybersecurity
3. Design a model for cybersecurity capacity building that takes into consideration all aspects (policy, technology, skills development)
4. Identifying areas of research needed for the formulation of policies, guidelines, etc., which can be general or sector-specific, for instance, cybersecurity for financial systems and for equipment monitoring tools.
5. Proactive Cyber Threat Hunting on Digital Government Infrastructure. The client must conduct regular tests for compliance with security policies and procedures to ensure security measures are protecting the organization.
6. Analyse and assess vulnerabilities in the infrastructure (software, hardware, networks), investigate available tools and countermeasures to remedy the detected vulnerabilities, and recommend solutions and best practices to protect against internal and external attacks.
7. Assist in the creation, implementation, and management of Security Solutions.
8. The firm must prepare reports for the client, detailing the weak security areas and make recommendations to rectify the problems.
9. Assist with the validation of the security posture of new changes to the Infrastructure of Government Network of Maldives and Digital Government Hosting Infrastructure and provide advice on changes to be brought.
10. Attending to incidents handling and response requested by the organization. Analyse and assess damage to the data/ Infrastructure as a result of security

incidents, examine available recovery tools and processes, and recommend a solution.

11. Where needed, the Firm should submit forensic evidence to identify patient zero of any incident handling and response case. The Firm should initiate the remediation process and propose recommendations to mitigate future threats. Discover indicators of compromise (IOCs) or create new IOCs from incident handling and response processes for cyber threat intelligence, which can be used for mitigations across the government in future as a reference on attacker patterns.
12. Alert the organization on new cyber threats and prepare advisory notices to be published `to the media.
13. Assist during the implementation process of the National Security Operations Center and the National Computer Emergency Response Team (CERT) at the NCIT.
14. Providing Source Code Audit for eGovernment Applications and assist in the implementation of automated static code analysis.
15. Audit the current policies, processes, and procedures of NCIT and assess whether the organisation is complying to them and recommend solutions to comply, or best practices to be able to comply with the policies.
16. Audit the IT Disaster Recovery Plan and its effectiveness.
17. Develop, maintain and providing support for the cybersafe.mv initiative
18. Reviewing DevSecOps automations of the infrastructure and providing best practice recommendations

Deliverables

1. The deliverables of the cyber security consultancy provider include:
2. Just-in-time technical assistance: This refers to providing technical support as and when required to deal with any cybersecurity-related issues that arise.
3. Quarterly Internal and External Penetration Testing: This involves conducting tests to identify vulnerabilities in the organization's internal and external systems.
4. Risk Assessment: This involves assessing and evaluating the risks associated with the organisation's systems, networks, and data to identify potential threats and vulnerabilities.
5. IT Security Policies: Developing policies and guidelines that outline best practices for the organisation's IT security and governance.

6. Overall Cyber Security Strategy and Work Plan: Developing a comprehensive strategy and work plan to address the organization's cybersecurity needs and objectives.
7. Support drafting of guidelines, regulations, and bylaws to assist the government in cyber security programs: Providing support in drafting guidelines, regulations, and bylaws to assist the government in implementing effective cybersecurity programs.
8. Proactive Cyber Threat Hunting on Digital Government Infrastructure and provide Indicator of Compromise (IOCs): Conducting proactive cyber threat hunting on the organisation's digital government infrastructure to detect and prevent cyber attacks. Providing IOCs to assist in identifying and mitigating cyber threats.
9. Support for the Cyber Security Awareness Programs: Providing support in the development and implementation of cybersecurity awareness programs to educate employees and stakeholders on best practices for ensuring IT security.
10. Incident Response Planning and Support: Developing incident response plans and providing support to the organization in responding to cybersecurity incidents effectively.
11. Compliance and Regulatory Support: Ensuring that the organization is compliant with relevant cybersecurity regulations and standards and providing support in obtaining necessary certifications and approvals.
12. Security Architecture Review: Conducting reviews of the organization's security architecture to identify potential vulnerabilities and recommending appropriate measures to enhance security.
13. Vendor Risk Management: Assessing and managing the risks associated with third-party vendors and suppliers to ensure that they meet the organization's cybersecurity standards and requirements.
14. Security Training and Awareness: Providing training and awareness programs to employees and stakeholders on the importance of cybersecurity and best practices for ensuring IT security.
15. Vulnerability Management: Identifying and prioritizing vulnerabilities in the organization's systems and networks and recommending appropriate measures to mitigate risks.
16. Forensic Investigations: Conducting forensic investigations to identify the root cause of cybersecurity incidents and to gather evidence for legal proceedings if necessary.

17. Cloud Security Assessment and Advisory Services: Assessing the security of the organization's cloud-based systems and providing recommendations for enhancing security.
18. Physical Security Assessment: Assessing the physical security of the organization's facilities to identify potential vulnerabilities and recommending appropriate measures to enhance security.
19. Application Security Testing: Conducting application security testing to verify the effectiveness of the code remediation and to ensure that the organization's software applications are secure and resilient against cyber attacks.
20. Continuous Monitoring and Assessment: Providing ongoing monitoring and assessment of the organization's software applications to ensure that any new vulnerabilities or weaknesses are identified and remediated in a timely manner.
21. Source Code Review: Conducting an in-depth review of the organization's software applications to identify potential security vulnerabilities and weaknesses in the code.

Experience and Skills:

1. Valid Certification: The personnel conducting the penetration testing and audit should have a valid certification from a trustworthy and industry well-known cyber security assessment certification body. This certification should demonstrate their expertise and knowledge in cybersecurity, including the latest industry standards and best practices.

2. Prior IT Security Audit Experience: The consultancy firm should have prior experience in conducting IT security audits, including experience in IT security audit of an organization of a size no smaller than 300 employees. This experience should demonstrate their ability to identify and address cybersecurity risks and vulnerabilities in complex and large-scale organizations.

3. Software Development and DevOps Infrastructure: The consultancy firm should have a developer with more than 3 years of experience in software development and DevOps infrastructure. This experience should demonstrate their ability to assess and test the security of software applications and infrastructure, as well as identify and address vulnerabilities in DevOps practices.

4. Enterprise IDP Experience: The consultancy firm should have a developer with experience of enterprise IDP (openid and oauth2). This experience should demonstrate their ability to assess and test the security of identity and access

management systems, as well as identify and address vulnerabilities in enterprise identity management practices.

5. Digital Forensics Experience: The consultancy firm should have a staff member with a minimum of 2 years of experience in digital forensics in incident handling and response with references. This experience should demonstrate their ability to investigate and respond to security incidents, as well as identify and recover from security breaches.

6. Enterprise Infrastructure Experience: The consultancy firm should have engineers with experience with a minimum of 3 years for enterprise infrastructure. This experience should demonstrate their ability to assess and test the security of complex and large-scale infrastructure, as well as identify and address vulnerabilities in enterprise infrastructure practices.

7. Compliance and Regulations Knowledge: The consultancy firm should have security professionals with experience in providing guidance and support to organizations on various cybersecurity regulations and frameworks, including but not limited to national cybersecurity frameworks. They should be able to assist the organization in understanding and implementing the framework's requirements, identify gaps in compliance, and recommend best practices for improving cybersecurity posture.

4. ސެލާން ހުރަހުގައި ބަލައިގަނެ ހުއްދަ ދިނުމުގެ ތަފްޞީލު.	
4.1.	ހުރަހުގެ ދާއިރާގެ ކުރިންވެސް
4.2.	ސެލާން ހުރަހުގެ
4.3.	ގާއިމްކުރަން ބޭނުންވާ ގޮތް / ތަކެތި ލިޔުއްވާ ފޯމު
4.4.	ތިރީގައިވާ ލިޔުންތައް ހުށަހަޅާ ފޯމާ ގުޅިގެން ހުށަހަޅަންވާ ލިޔުންތައް (ކޮޕީ / ފޮޓޯ ސްޓޭޓް / ސްކޭން)
4.5.	ފިހާރަ ހިންގުމަށް ލިބިގެންވާ ލައިސަންސް ހުށަހަޅަންވާ ގޮތް.
4.6.	ފިހާރަ ހިންގުމަށް ލިބިގެންވާ ލައިސަންސް ކަމަށް ހަމަ ދުވަސް ގަޑިތަކުގައި ކަންތައް ކުރުމަށް ހުށަހަޅާ ތަނުގެ ތަފްޞީލު (ހ.ހުޅުވާނގު ތަނުގެ ލައިސަންސް) - ތަނުގެ ބޮޑުކަން ގަޑިތަކުން ގަޑިއިރަކަށް
4.7.	ފެންވަސް ތަކެތި ތަނުގައި ބެހެއްޓުމަށް ހުށަހަޅާ ތަނުގެ ބޮޑުކަން ސްކެއާ ފޫޓްގައި ލިޔުއްވާ ގޮތް
4.8.	ފެންވަސް ތަކެތި ތަނުގައި ބެހެއްޓުމަށް ހުށަހަޅާ ތަނުގެ ލޭއުޓް ތަކެތި ލިޔުއްވާ ގޮތް (ލޭ.ހުޅުވާނގު ތަނުގެ ލައިސަންސް ކަމަށް)
4.9.	ފެންވަސް ތަކެތި ތަނުގައި ބެހެއްޓުމަށް ހުށަހަޅާ ތަނުގެ ބޮޑުކަން ކްލައިމް ކުރާ ގޮތް (ދުވަސްތަކުގެ 03 ގަޑު ކަމަށްވާ)
4.10.	ގަސްތަކުގެ ބަދަލުގައި ހަރުކަށި ބަދަލުތައް ފަރުނީޗަރ ގަތުމަށް ގަސްތަކުގެ ބަދަލުގައި ހުށަހަޅަންވާ ގޮތް
4.11.	ފާރ ފުރުތަކުގައި ކަނޑައެޅިފައިވާ ސަރުކާރުގެ ކަންކަމާ ގުޅުންހުރި ތަކެތި ވިއްކާ ތަނެއް "ގާއިމްކުރަން ހުއްދަ ދިނުމުގެ ގޮތުގެ ގާނޫނު" ގެ ދަށުން ހުށަހަޅާ ދާއިރާގެ ބޮޑުކަމުގެ ސަރުވޭ ކުރެވިފައިވާ ގޮތް، 2019 ، 2020 ގެ 2021 ގެ ކުރިން ގަސް ތަކެތި ލިޔުއްވާ ގޮތް) ތަކެތި ލިޔުއްވާ ގޮތް (ދުވަސްތަކުގެ 03 ގަޑު 03)

Marking Criteria

1.1 Marking Criteria for Price

- Lowest bid / bid price × 55 among the bidders

1.2 Marking Criteria for Experience and Team Qualification.

- 5 points will be awarded for each reference document submitted that meets the following requirements. The maximum score for this section is 45 points.

#	Documents	Marks
1	**Valid Certification:** The personnel conducting the penetration testing and audit should have a valid certification from a trustworthy and industry well-known cyber security assessment certification body. This certification should demonstrate their expertise and knowledge in cybersecurity, including the latest industry standards and best practices.	
2	**Prior IT Security Audit Experience:** The consultancy firm should have prior experience in conducting IT security audits, including experience in IT security audit of at least 03 organizations of a size no smaller than 300 employees. This experience should demonstrate their ability to identify and address cybersecurity risks and vulnerabilities in complex and large-scale organizations.	
3	**Software Development and DevOps Infrastructure:** The consultancy firm should have a developer with more than 3 years of experience in software development and DevOps infrastructure. This experience should demonstrate their ability to assess and test the security of software applications and infrastructure, as well as identify and address vulnerabilities in DevOps practices.	
4	**Enterprise IDP Experience:** The consultancy firm should have a developer with experience of enterprise IDP (openid and oauth2). This experience should demonstrate their ability to assess and test the security of identity and access management systems, as well as identify and address vulnerabilities in enterprise identity management practices.	
5	**Digital Forensics Experience:** The consultancy firm should have a staff member with a minimum of 2 years of experience in digital forensics in incident handling and response with references. This experience should demonstrate their ability to investigate and respond to security incidents, as well as identify and recover from security breaches.	
6	**Enterprise Infrastructure Experience:** The consultancy firm should have local engineers with experience with a minimum of 3 years for enterprise infrastructure. This experience should demonstrate their ability to assess and test the security of complex and large-scale infrastructure, as well as identify and address vulnerabilities in enterprise infrastructure practices.	
7	**Compliance and Regulations Knowledge:** The consultancy firm should have security professionals with experience in providing guidance and support to organizations on various cybersecurity regulations and frameworks, including but not limited to national cybersecurity frameworks. They should be able to assist the organization in understanding and implementing the framework's requirements, identify gaps in compliance, and recommend best practices for improving cybersecurity posture.	
TOTAL MARKS		

1.3 Total Marking Criteria for Evaluation

#	Marking Criteria's	Marks	Description
1	Price	55%	Lowest bid / bid price × 55 among the bidders
2	Experience and Team Qualification.	45%	Total marks of 1.2 Marking Criteria for Experience and Team Qualification / 35 x 45

5. ތަކެއްޗާ ގުޅޭ ހިންގުމުގެ ގޮތް ފުރިހަމަކުރުން

- ހިނގާ ހަފްތާ ތެދުވާ ދުވަހުގެ ކުރިން ކުރިއަށް ގެންދާ ތަރައްޤީ ހިނގާ ގޮތް ބަލައި ބަލައިގަތުން.
- ހިނގާ ކުރިއަށް ގެންދާ ތަރައްޤީ ބަލައި ގަތުމުގެ ދަށުން ކުރިއަށް ގެންދާ ތަރައްޤީ ބަލައި ގަތުމުގެ ރިޕޯޓް ތައްޔާރުކުރުން.
- ފާސްކުރެވިފައިވާ ބަޖެޓް ހިންގުމުގެ ދަށުން 2019، 2020 ، 2021 ވަނަ ހަ ހަފްތާ ތެދުވާ ދުވަހުގެ ތެދުވުންތަކުގައި ކުރިއަށް ގެންދާ ތަރައްޤީ ހިނގާ ގޮތް ބަލައި ގަތުމުގެ ދަށުން ތައްޔާރުކުރެވޭ ރިޕޯޓް ތަކުގައި ހިމެނޭ ގޮތަށް ތަކެއްޗާ ގުޅޭ ހިންގުމުގެ ރިޕޯޓް ތައްޔާރުކުރުން.
- ކުރިއަށް ގެންދާ ތަރައްޤީ ބަލައި ގަތުމުގެ ދަށުން ތައްޔާރުކުރެވޭ ރިޕޯޓް ތަކުގެ ތެދުވުންތަކުގައި ކުރިއަށް ގެންދާ ތަރައްޤީ ބަލައި ގަތުމުގެ ކޮމިޓީ ގެ ކަންތައް ކުރުން.
- ކުރިއަށް ގެންދާ ތަރައްޤީ ބަލައި ގަތުމުގެ ކޮމިޓީ ގެ ކަންތައް ކުރުން.

6.1. ހުށަހަނާ ފަރާތުގެ ތަފްޞީލު

National Centre for Information Technology

ކުށަހަނާ ގޮތުގައި ފޯމު ހިއްދުމަށް

#	ހުށަހަނާ ބިރުދޭ ފަރާތް	ސޮފްޓް	ފުރަތަ
1	ހުށަހަނާ ފަރާތުގެ ތަފްޞީލު		
2	ކާނާ ހުށަހަނާކުރި		
3	ގަބޫލުކުރާ ވަކި ދުވަހެއް / ދުވަސް ތެރެ ފަރާތަށް ހުށަހަނާ ކުށް		
4	ބިލްގައި ދައްކާ ގޮތް ތަފާތުވާ ވިދާލައިގެން ދިނުމަށް. (ކާނާ / ފާރަސް / ކާބޯތަކެއް / ތަކެތި ސަޕްލައި / ތަރުތީބު ފަދަ ކަންތައްތަކުގައި ތަފާތު ދައްކާ ގޮތް ކަށަވަރު ކުރުން)		
5	ފިޔަވަޅު ކަނޑާ ތާށިވުމުގެ ދަށުން ދަތުރުގައި ހުންނަ ފަރާތަށް ދިނުމަށް.		
6	ފިޔަވަޅު ކަނޑާ ތާށިވުމުގެ ދަށުން ދަތުރުގައި ހުންނަ ފަރާތަށް ދެ ދުވަހުގެ ތެރޭގައި ވިދާލައިގެން ދިނުމަށް ފަރާތުގެ ވިދާލައިގެން ދިނުމަށް (ދަތުރުގައި ހުންނަ ދުވަސްތަކުގެ ތެރެއިން ދެ ދުވަހުގެ ތެރޭ) - ތަފާތު ދައްކާ ގޮތް		
7	ފާސްޓްފޫޑް ރެސްޓޯރާ ތިމާވެއްޓާ ބައްދަލުކުރާ ގޮތުގައި ކާނާ ތަފާތު ދައްކާ ގޮތް ކަށަވަރު ކުރުން		
8	ފާސްޓްފޫޑް ރެސްޓޯރާ ތިމާވެއްޓާ ބައްދަލުކުރާ ގޮތުގައި ކާނާ ތަފާތު ދައްކާ ގޮތް ކަށަވަރު ކުރުން (ކާ.ބޯ.ސާ.ތަކެތި ތަފާތު ދައްކާ ގޮތް ކަށަވަރު ކުރުން)		
9	ފާސްޓްފޫޑް ރެސްޓޯރާ ތިމާވެއްޓާ ބައްދަލުކުރާ ގޮތުގައި ކާނާ ތަފާތު ކަމުގައި ބެލެނިވޭ ކަންތައް (ބައްދަލުކުރާ 03 ދަނޑު ހަދާފައި)		
10	ދަނޑުތަކުގެ ތަރުތީބުތަކާ ހަދާފައިވާ ގޮތުގައި ކާނާ ތަފާތު ދައްކާ ގޮތް ކަށަވަރު ކުރުން		
11	ފަރާތުގެ ކާބޯތަކާ ގުޅިގެން ކާނާ ތަފާތު ދައްކާ ގޮތް ކަށަވަރު ކުރުމަށް "ގަބޫލުކުރާ ވަކި ދުވަހެއް" ތެރެ ދަތުރުގައި ހުންނަ ދުވަސްތަކުގެ ތެރެއިން ދެ ދުވަހުގެ ތެރޭ (2019، 2020 ތެރެ 2021 ވަނަ ހަފްތާ ފަރާތުން ހުށަހަނާ ކުށްތަކަށް) ދަތުރުގައި ހުންނަ ފަރާތަށް ދެ ދުވަހުގެ ތެރޭ ކާނާ ދިނުމަށް (ދެ ދުވަހަށް 03 ފަހަރު 03)		

6.2 ތަކެއްގެ ހުށަހެޅުން

National Centre for Information Technology

ދާއިރާގެ ގޮތުގައި ކުރިއަށް ގެންދާ ތަރައްޤީ ޕްރޮޖެކްޓް ތަކުގެ ތަފްޞީލް

ތަކެއްގެ ނަންބަރު:		ވަގުތު:	
ތަކެއްގެ ގުޅުން ހުރި ކޮންމެ ކޮންޓްރެކްޓެއް ނުވަތަ ކުންފުނި ނަންބަރ			
ނަން:			
ތަކެއްގެ ނަންބަރ:			
ދަށ:			
ގުޅުން ނަންބަރ:			
ތާރީޚ:			
ވަގުތު:			
ސަބަބު:			
ތ ތަކެއްގެ ކުންފުނިގެ ސްޓާފުން ބަދަލުކުރާ ފަރާތް ކަނޑައަޅާ ތާރީ ތަކެއްގެ ގުޅުން ހުރި ކޮންމެ ކޮންޓްރެކްޓެއް ނުވަތަ ކުންފުނ ތަކެއްގެ ގުޅުން ހުރި ކޮންމެ ކޮންޓްރެކްޓެއް ނުވަތަ ކުންފުނ			
ތަކެއްގެ ކުންފުނި (ތަނުގެ ގުޅުން ހުރި ކޮންމެ ކުންފުނ ސަބަބު ދެއްކުމަށް ބޭނުންވާ ތަކެއ			
ނަން:			
ދަށ:			
ގުޅުން ނަންބަރ:			
ތާރީޚ:			
ވަގުތު:			
ސަބަބު:			

6.2. ފަރާތްތަކުގެ ބޭނުމަށް ގުޅި (ފިހާ ގުޅި-1) ތަކެއް ގުޅުވައިދިނުމަށް ބަދަލުގައި ދައްކަންޖެހޭ ފައިސާ ކޮންސަލްޓަންސީ ސާރވިސް ފީ ހިންގުމަށް ގުޅި ތަކެއް ލިބިގަތުމުގެ ކުރިން ދައްކަންޖެހޭނެ ގޮތް ކަނޑައަޅާ ބަޔާންކުރުން. ތަކެއް ލިބިގަތުމުގެ ކުރިން ދައްކަންޖެހޭ ފައިސާ ދައްކާ ގޮތް ކަނޑައަޅާ ބަޔާންކުރުން.

بسم الله الرحمن الرحيم

National Centre for Information Technology

ކޮންސަލްޓަންސީ ސާރވިސް ފީ ހިންގުމަށް

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

Description	Months	Monthly Rate	GST (8%)	Total Amount with GST
Consultant Fee per month	Month - 1			
	Month - 2			
	Month - 3			
	Month - 4			
	Month - 5			
	Month - 6			
	Month - 7			
	Month - 8			
	Month - 9			
	Month - 10			
	Month - 11			
	Month - 12			
	Total (Yearly)			

Bidder Stamp and Sign

_____

6.3 ފަރާތްތަކުގެ ފައިނޭންސް ޑޭޓާ (ފޮށި ގުޑު-2)

National Centre for Information Technology

ދާއިރާގެ ގޮތުގައި ބަލާ ލިބިދާނެ ފައިސާ

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 900,000.00 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 900,000.00 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 900,000.00 of the proposed price)

Bidder Stamp and Sign

_____

6.4 ފަރާތް ހޮޅުވާ ކަމުގެ ލިޔުން

[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:

6.5. ހުއްދަ ދޫކުރުން

ހުއްދަ

ތަރުތީބު:

1.	ތަފާތު.	1.1. ދިވެ (ދަތުރުކުރާ ތަކެތި) ގެންދާނަމަ ދަތުރުގައި ހުންނަ ބަޔަކު ހުއްދަ ދޫކުރަންވާނެ.
2.	ހުއްދަ ދޫކުރާ ތަނެވަސް.	2.1. ދި ހުއްދަ ދޫކުރާނީ ދާދަތަކުން ގެންދާ ތިމާވެށި ތަކެތި ބަލައިގަތުމަށް ކަމުގައި ވާ ތަނެވަސް ކަމަށެވެ.
		2.2. ދަތުރުކުރާ ފަރާތް ގަބޫލު ކުރާ ތަނެވަސް (ކުންފުނި ނުވަތަ ވިއަފާރިގެ ނަން)
3.	ހުއްދަ ދޫކުރާ ތަނުގެ ހަގީގީ ދަތުރުކުރާ ބަޔަކު	3.1. ދަތުރުކުރާ ފަރާތް ގެންދާ ތަކެތި (ތަކެތީގެ ނަންތައް) ބަލައިގަތުމަށް ފަހު ތަކެތި ގެންދާ ފަރާތް ދިރާސާ ކުރާނެ ގޮތް (ދި ހުއްދަ ދޫކުރާ 1 ވަނަ ތަނުގައި ބަލައިގަންނަ ތަކެތި ތިރީގައި ބަލައި ހުންނަ/ދަތުރުކުރާ ފަރާތް ގެންދާ ތަކެތި ބަލައިގަތުމަށް ކުރިން ބަލާ ގޮތް)
4.	ދަތުރުކުރާ ދުވަސް.	4.1. ތިރީގައި 1 ވަނަ ދަތުރުކުރާ ދުވަސް ދަތުރުކުރާ ދުވަސް (ދުވަސް) ހުއްދަ ދޫކުރާ ތަނެވަސް ކަމަށެވެ.
5.	ދަތުރުކުރާ ދުވަސް.	5.1. ތިރީގައި 1 ވަނަ ތާރީޚުގައި ދަތުރުކުރާ (ދުވަސް) ދުވަހުގެ ތެދުވާ ގޮތް (ތަފްޞީލު ކުރާ ގޮތަށް ބަލައި) ކުންފުނި ދަތުރުކުރާ ތަނެވަސް ހުއްދަ ދޫކުރާ ގޮތް ކަމަށެވެ.
		(ހ) ހުއްދަ ދޫކުރާ ތަނުގެ ނަން (ފަރާތް) ކަމަށެވެ.
		(ށ) ހުއްދަ ދޫކުރާ ތަނުގައި ދަތުރުކުރާ ދުވަސް (ފަރާތް) ކަމަށެވެ.
6.	ދަތުރުކުރާ ގޮތް ބަލައިގަތުން	6.1. ދަތުރުކުރާ ހުއްދަ ދޫކުރާ ގޮތް ކުންފުނި ދަތުރުކުރާ ތަކެތި ދަތުރުގައި ގެންދާ ގޮތް، ދަތުރުކުރާ ތަކެތި ދަތުރުގައި ގެންދާ ގޮތް، ދަތުރުކުރާ ތަކެތި ގެންދާ ގޮތް ބަލައިގަތުމަށް ކުރިން ދަތުރުކުރާ ފަރާތް ގެންދާ ތަކެތި ބަލައި ހުންނަ ގޮތް ކަމަށެވެ. ތަކެތި ދި ހުއްދަ ދޫކުރާ ދުވަހުގެ 30 (ތިރީސް) ދުވަހުގެ ތެދުވާ ގޮތަށް ކަމަށެވެ.

.7 ނިންމަންވީ ގޮތާއި ފެންވަރު

.7.1 ކުރަންޖެހޭ މަސައްކަތްތަކުގެ ތަފްސީލު، މި އެއްބަސްވުމުގެ ޖަދުވަލު 1 ގައި ބަޔާން ކުރެވިފައިވާނެއެވެ. އަދި މި މަސައްކަތް ޖަދުވަލު 1 ގައި ބަޔާންކޮށްފައިވާ ފެންވަރާއި ވަގުތަށް ނިންމަންވާނެއެވެ.

.7.2 ކަނޑައަޅާފައިވާ މުއްދަތުގެ ތެރޭގައި މަސައްކަތް ހަވާލުކުރި ފަރާތަށް ޤަބޫލު ކުރެވޭފަދަ ރަނގަޅު ފެންވަރެއްގައި މަސައްކަތް ނިންމުމަށްފަހު މަސައްކަތް ހަވާލުކުރި ފަރާތާ ހަވާލު ކުރަންވާނެއެވެ.

.8 މަސައްކަތަށް ބަދަލުގެނައުން.

.8.1 މި އެއްބަސްވުމުގައި ކުރުމަށް ޖަދުވަލު 1 ގައި ބަޔާންކުރެވިފައިވާ މަސައްކަތްތަކަށް އެއްވެސް ބަދަލެއް (އަގު، މުއްދަތު ނުވަތަ މަސައްކަތައް) ގެންނަން ޖެހިއްޖެ ނަމަ ހިދުމަތް ދޭ ފަރާތުން ނުވަތަ ހިދުމަތް ލިބިގަންނަ ފަރާތުން ލިޔުމަކުން އެގްރިމަންޓްގެ މުއްދަތުގައި އަންގައި ހުއްދަ ހޯދަން ވާނެއެވެ.

(ހ) މި އެއްބަސްވުމުގެ ޖަދުވަލު 1 ގައި ބަޔާންކޮށްފައިވާ މަސައްކަތްތަކުގެ އިތުރުން މަސައްކަތެއް ކުރަން ޖެހިއްޖެނަމަ މަސައްކަތް ހަވާލުކުރާފަރާތުން މަސައްކަތުގެ ސްކޯޕް ލިޔުމުން ފޯރުކޮށްދޭންވާނެއެވެ.

(ށ) ސްކޯޕް ކަވަރުނުވާ ކަންކަމަށް، މަސައްކަތް ކުރާ ފަރާތުން އެކަމަށް ހިނގާނެ ހަރަދު ބަޔާންކޮށް ލިޔުމުން މަސައްކަތް ހަވާލުކުރި ފަރާތަށް ހުށަހަޅަންވާނެއެވެ.

(ނ) މިގޮތުން އިތުރުކުރާ މަސައްކަތް ކުރަންވާނީ ދެފަރާތުން އެއްބަސްވުމެއް ހަދައި އެއްބަސްވުމުގައި ސޮއިކުރުމަށްފަހުއެވެ.

(ރ) އަގަށް އެއްބަސް ނުވެވޭ ހާލަތްތަކުގައި އެހެން ފަރާތްތަކާއި އެކު މަސައްކަތުގެ އެއްބަސްވުން ހެދުމުގެ އިޚްތިޔާރު، މަސައްކަތް ހަވާލުކުރާ ފަރާތަށް ލިބިގެންވެއެވެ.

(ބ) ކަނޑައެޅިފައިވާ މުއްދަތަށް މަސައްކަތް ނިންމުމަށް މަސައްކަތް ހަވާލުވި ފަރާތަށް ދަތިވާނަމަ ސަބަބު ބަޔާންކޮށް މަސައްކަތް ހަވާލުކުރިފަރާތުން ބަޔާންކުރާ ޑެޑްލައިނާއި ދުވަހާއި ލިޔުމުން އަންގަންވާނެއެވެ.

8.2. ލިޔުމުން ހުށަހަ ތަފާތުތައް ކަނޑައެޅުމުގެ ކުރިން ކޮންޓްރެކްޓް ހަވާލުކުރާ ބޭނުންވާ ތަނުގައި 10.55 ގަޑި ހުއްދަ ދިނުމަށް ބެލެހެއްޓުން.

8.3. ލި ތާރީޚުގެ ކުރިން ހުށަހެޅުން.

9. ކަންތައް ހުއްޓާލުމުގެ ފުރިހަމަ ކުރުމުގެ ތަކެތި.

9.1. ލިޔުމުން ހަނގުރާ ކަންތައް ހުއްޓާލުމުގެ ތަކެތި ކުރިން ހުށަހަޅާ ކޮންޓްރެކްޓް ލިބިގެންދާ ފަރާތަށް ކުރިއަށް ގެންދާ ކަންތައް ހުއްޓާލުމަށް ބޭނުންވާ ތަކެތި ހުށަހަޅަންވާނެ.

9.2. ކޮންޓްރެކްޓް ދިނުމުގެ ކަންތައް ފުރިހަމަ ކުރުމަށް ހަނގުރާ ކަންތައް ހުއްޓާލުމުގެ ތަކެތި ހުށަހަޅާ ތާރީޚުގެ ފަހުން 10.71 ގަސް ފާރުގެ ގަދަ ކަންތައް ދިނުމުގެ ކުރިން ކަނޑައެޅިފައިވާ ތަނަށް ގެންދިއުމަށް ބޭނުންވާ ތަކެތި ހުށަހަޅަންވާނެ.

9.3. ދުވަހަކަށް 5,000,000/- ރުފިޔާގެ ދަށުން ކަނޑައެޅިފައިވާ ގަޑިއިން ގަޑިއަށް ކަންތައް ހުއްޓާލުމުގެ ދުވަހަކަށް 0.005 (ފަސްދިހަ ހާސަތު ފަސް ދިހަ ލައްވާ) ގެ ފަސާރަމަތީގައި ދުވަހުގެ ތަކެތި ހުށަހަޅާ ގަޑި ކަނޑައެޅުން.

ލިބުމަށްޓަކާ ގެންދާ ތަކެތި = CP*0.005*LD

ތަނަކީ 5,000,000/- ރުފިޔާގެ ދަށުން ކަނޑައެޅިފައިވާ ތަނެއް ނަމަ ދުވަހަކަށް 0.0025 (ފަސްދިހަ ހާސަތު ފަސް ހާސް ލައްވާ) ގެ ފަސާރަމަތީގައި ދުވަހުގެ ތަކެތި ހުށަހަޅާ ގަޑި ކަނޑައެޅުން.

ލިބުމަށްޓަކާ ގެންދާ ތަކެތި = CP*0.0025*LD

CP (ކޮންޓްރެކްޓް ވެލަދެވޭ): ކޮންޓްރެކްޓުގެ ދުވަހަކަށް

LD (ފުރިހަމަ ކުރުމުގެ): ކޮންޓްރެކްޓުގެ ދުވަހަކަށް ހަނގުރާ ކަންތައް ހުއްޓާލުމުގެ

9.4. • ލި ތާރީޚުގެ ފަހުން ކަނޑައެޅިފައިވާ ތަނަށް ގެންދާ ތަކެތި ދުވަހުގެ ކަނޑައެޅުމުގެ ގަޑިއިން (ދުވަހުގެ ތަކެތި) ކޮންޓްރެކްޓުގެ ފުރިހަމަ ކުރުމަށް.

9.5. ގެންދާ ތަކެތި ގެންދާ ގަޑި ކަނޑައެޅިފައިވާ ތަނުގައި ދުވަހަކަށް ކުރިން ކަނޑައެޅުމުގެ 15% (ފަސްދިހަ ފަސް ސައްވަ) ދުވަހުގެ ދަށުން ދައްކަންވާނެ.

9.6. ކަންތައް ހުއްޓާލުމުގެ ގަޑި ކަނޑައެޅުމުގެ 15% (ފަސްދިހަ ފަސް ސައްވަ) ދުވަހުގެ ތަކެތި ލިބުމަށްޓަކާ ގެންދާ ގަޑި ކަނޑައެޅުމުގެ ދުވަހަކަށް، ކޮންޓްރެކްޓުގެ ދުވަހުގެ ތަކެތި ލިބުމަށްޓަކާ ގެންދާ ގަޑި ކަނޑައެޅުމުގެ ދުވަހުގެ ތަކެތި ލިބުމަށްޓަކާ ގެންދާ ގަޑި ކަނޑައެޅުން. ތަނުގައި ކޮންޓްރެކްޓަރ ހުއްޓާލާ ގެންދާ ކަންތައް

ފަރާތްތަކުން ކުރިއަރުވާ ކަންތައް ހުއްދަ ދިނުމުގެ ކުރިން ކުރިއަރުވާ ފަރާތަށް ދަންނަވައި ބަލައިގަތުމަށް ފުރުޞަތު ދިނުން.

9.7. ހިއްސާދާރުންގެ ބަދަލުގައި ކުރިއަރުވާ ފަރާތަށް ހުއްދަ ދިނުމުގެ ކުރިން ހިއްސާދާރުންގެ ގާތް ހިއްސާ ގަނެ ނިންމުން.

10. ހުއްދަ ކެންސަލް ކުރުމުގެ 10.1. ހިއްސާދާރުންގެ ކުރިއަރުވާ ހިއްސާ ކުރިން ހުއްދަ ދީފައިވާ ހިއްސާ ކަނޑައެޅުމުގައި ބަދަލުވެ ދިއުން ހުއްދަ ދީފައިވާ ފަރާތަށް ދަންނަވައި ކެންސަލް ކުރުން. ހުއްދަ ދީފައިވާ ފަރާތަށް ދަންނަވައި ކެންސަލް ކުރުމުގެ ކުރިން ހުއްދަ ދީފައިވާ ފަރާތަށް ދެއްކި ފައިސާ ފަރާތަށް ދެއްކުން.

11. ދިވެހިންގެ ގޮތުގައި ކުރިއަރުވާ ފަރާތް 11.1. ދިވެހިންގެ ގޮތުގައި ކުރިއަރުވާ ފަރާތަށް ދަންނަވައި ކުރިއަރުވާ ކަންތައް ދިވެހި ބަހުގައި ލިޔެ ހުށަހެޅުން.

12. ދުވަސްވަރުގެ ކަންކަން. 12.1. ހިއްސާދާރުންގެ ފާހަގަ ކުރެވިފައިވާ ހުއްދަ ދީފައިވާ ތަނުގައި ހުއްދަ ދީފައިވާ ތަނުގައި ކުރިއަރުވާ ކަންތައް ދުވަހުގެ ތެދުވެރިކަމާ ގުޅޭ ގޮތުން ކުރިއަރުވާ ފަރާތަށް ދަންނަވައި ބަލައިގަތުމަށް ފުރުޞަތު ދިނުން.

ދަނޑިފަރާތް ކުރިއަރުވާ ކަންތައް ހުއްދަ ދީފައިވާ ފަރާތުން (ވަކީލު) ވ (ފުރަހަ) ފުރަތަށް ބަދަލުކުރުމުގެ ކުރިން ބަދަލުކުރުމަށް ދަންނަވައި ބަލައިގަތުމަށް ފުރުޞަތު ދިނުން.

ހުއްދަ ދީފައިވާ ފަރާތް	ހުއްދަ ދީފައިވާ ފަރާތަށް
(ހުއްދަ ދީފައިވާ ފަރާތުގެ ސަހީ)	(ހުއްދަ ދީފައިވާ ފަރާތަށް ސަހީ)

ސަހީ :

ސަހީ :

ނަން :

ހުއްދަ ދީފައިވާ ފަރާތަށް

ދަސްވެހި ހަރަކާތްތެރި ފަރާތް	ދަސްވެހަށް ހަރަކާތްތެރި ފަރާތް
ނަން:	ނަން:
ކަނޑަށް:	ކަނޑަށް :
ތާރީޚް :	ތާރީޚް :