بسم الله الرحمن الرحيم

ދާއިރާގެ ކުންފުނި ލިމިޓެޑް ތިރީ ތަކެއްޗާ ގުޅޭ

ދަރަނި ގަވާ

ގަވާ ކުރާ ތަކެއްޗާ ގުޅޭ ތަފްޞީލް	ދާއިރާގެ ކުންފުނި ލިމިޓެޑް ތިރީ ތަކެއްޗާ ގުޅޭ ގަވާ ކުރާ ތަކެއްޗާ ގުޅޭ ތަފްޞީލް
ގަވާ ކުރާ ނަންބަރ	PROC-2023-015
ބިޑް ނަންބަރ	**(IUL)164-PRO/1/2023/40**
ތާރީޚް	05 ފެބްރުވަރީ 2023

1. ބީލަމާއި ގުޅޭ އާންމު މައުލޫމާތު		
1.1. ތައާރަފު	މިއީ މިއިދާރާއަށް ގަންނަން ބޭނުންވާ/ ހިދުމަތެއް ހޯދުމަށް ކުރެވޭ އާންމު އިއުލާނެކެވެ.	
1.2. އިއުލާން	ނަންބަރު	(IUL)164-PRO/1/2023/40
	އިއުލާން ތާރީހު	05 އޮކްޓޫބަރު 2023
	ބީލަމުގެ ނަން	ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ އަށް ސައިބަރ ސެކިއުރިޓީ ކޮންސަލްޓެންސީ ފްރޭމްވަރކް
1.3. ބީލަން ހުށަހެޅުން	ތަން	ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ
	އެޑްރެސް	NCIT ބިލްޑިންގ، 64 ނިކަ ގޯޅި، ކަލާފާނު ހިނގުން
	ތާރީޚާއި ގަޑި	2023 އޮކްޓޫބަރު 26 ވާ ބުދަ ދުވަހުގެ 11:00 ގެ ކުރިން NCIT ގެ ރިސެޕްޝަނަށެވެ. ގަޑިޖެހުމަށްފަހު ހުށަހަޅާ ބީލަމެއް ބަލައި ނުގަންނާނެއެވެ. އަދި އެއްވެސް ސަބަބަކާހުރި މުއްދަތު (2023 އޮކްޓޫބަރު 26 ވާ ބުދަ) ބަންދުނަމަ، ޤަވާއިދުން އަންނަ ރަސްމީ ދުވަހު 11:00 ގެ ކުރިން NCIT ގެ ރިސެޕްޝަނަށް ބީލަން ހުށަހަޅަންވާނެއެވެ. އަދި ގަޑިޖެހުމަށްފަހު ހުށަހަޅާ ބީލަމެއް ބަލައި ނުގަންނާނެއެވެ.
1.4. ބީލަން ހުޅުވުން	ތަން	ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ
	އެޑްރެސް	NCIT ބިލްޑިންގ، 64 ނިކަ ގޯޅި، ކަލާފާނު ހިނގުން
	ތާރީޚާއި ގަޑި	2023 އޮކްޓޫބަރު 26 ވާ ބުދަ ދުވަހު 11:10 ގައި، މި މަސައްކަތަށް އަންދާސީ ހިސާބު ހުށަހަޅުއްވާ ފަރާތްތަކުގެ ތަމްސީލުން އެވަގުތަކު ހާޒިރުވާ މީހުގެ ބީލަންވެރިން ނުވަތަ ބީލަންވެރިންގެ ބަދަލުގައި އެ ފަރާތްތަކުން ކަނޑައަޅާ ފަރާތްތަކުގެ ހާޒިރުގައެވެ. އަދި އެއްވެސް ސަބަބަކާހުރި މުއްދަތު (2023 އޮކްޓޫބަރު 26 ވާ ބުދަ) ބަންދުނަމަ، ޤަވާއިދުން އަންނަ ރަސްމީ ދުވަހު 11:10 ގައި، މި މަސައްކަތަށް އަންދާސީ ހިސާބު ހުށަހަޅުއްވާ ފަރާތްތަކުގެ ތަމްސީލުން އެވަގުތަކު ހާޒިރުވާ މީހުގެ ބީލަންވެރިން ނުވަތަ ބީލަންވެރިންގެ ބަދަލުގައި އެ ފަރާތްތަކުން ކަނޑައަޅާ ފަރާތްތަކުގެ ހާޒިރުގައެވެ.

·2 ފަރާތްތަކުން ހުށަހަޅަންޖެހޭ ކަނޑައެޅިފައިވާ ތަފާސީލާއި ލިޔެކިޔުންތައް	
·2·1	ހ. ވަޒަންދާ ގައުމީ ބޭންކުގެ ލައިސަންސް ހުންނަ ކުންފުނި / ކަނޑައެޅުނު ލައިސަންސް ހުންނަ ހ. ވަޒަންދާ ގައުމީ ބޭންކުގެ 3 ގަނޑު ތަކެއް ހުށަހަޅަންވާނެ.
·2·2	ވިލާގެ ބަންދުގެ ތަފާސީލު ދަންނަވަންވީ ކުންފުނީގެ 2023 ފެब्रުވަރީ 12 ވަނަ ބުރާސްފަތި 11:00 ގެ ކުރިން tender@ncit.gov.mv ގަށަވަރު. ތަނާ ބެހޭ ތަފާސީލުތައް ބަލައި ގަތުމުގެ ކުންފުނީގެ ނަމުގައި www.ncit.gov.mv ގައި 2023 ފެब्रުވަރީ 17 ވަ ވަނަ ބުރާސްފަތި 13:00 ގަނޑު ވިލާ ހުށަހަޅާ ފަރާތްތަކުގެ ކުރީގެ ލިޔުންތަކާ ތަފާސީލު ހުށަހަޅާ ފަރާތްތަކުގެ ކުންފުނީގެ ލެޓަރ ހެޑްގައި ލިޔެ ހުށަހަޅަންވާނެ. ވ. ވިލާ ހުށަހަޅާ ފަރާތްތަކުގެ ކުންފުނީ ރަޖިސްޓްރީ ކުރެވިފައި ހުންނަ ގަނޑު ތަކެއް ހުށަހަޅަންވާނެ.
·2·3	ވިލާ ކުރަންދާ ގަނޑު ތަކެއް (ކުންފުނީ ކުރިއަށް ގެންދާ ގަނޑު ތަކެއް) (ހ) ދިވެހި ރުފިޔާ ތަނަވަސް ކުންފުނިތަކަށް ދިވެހި ރުފިޔާ ދަށްކުރާ ގަނޑު ތަކެއް. (ށ) ފުރިހަމަ ތަފާސީލު ހުށަހަޅާ ތަނަވަސް ކުންފުނިތަކަށް ގަނޑު ތަކެއް.
·2·4	ވިލާ ކުރަންދާ ގަނޑު ތަކެއް، ވާދަކުރުމުގެ ގަނޑުގައި ދިވެހިރާއްޖެ ގައުމީ ބޭންކުގެ ވިލާ ގަނޑު ތަކެއް ހުންނަ ކަމަށް ބަލައި ދެވޭ ތަފާސީލު ހުށަހަޅަންވާނެ.
·2·5	ކުންފުނީ ކުރިއަށް ގެންދާ ކަނޑައެޅުނު ކޮންޓްރެކްޓް ގަނޑު ވިލާ ހުށަހަޅާ ފަރާތްތަކުން ހުށަހަޅަންވާ ލިޔުންތައް. ތަނާ ބެހޭ ވިލާ ހުށަހަޅާ ފަރާތްތަކުގެ ކުންފުނީ ކުރިއަށް ގެންދާ ކަނޑައެޅުނު ކޮންޓްރެކްޓް ގަނޑު ތަކެއް ހުށަހަޅަންވާނެ.
·2·6	ވިލާ ކުރަންދާ ގަނޑު ތަކެއް ލައިސަންސް ހުންނަ ކުންފުނީ ކަނޑައެޅުނު ގަނޑު ތަކެއް ހުށަހަޅަންވާނެ.
·2·7	ވިލާ ހުށަހަޅާ ފަރާތްތަކުގެ ފަރާތްތަކުގެ ލިޔުންތަކުގައި ދައްކާ ގަނޑު ތަކެއް ހުށަހަޅަންވާނެ. (ހ) ފަރާތްތަކުގެ ކުންފުނީ ސާފުކުރެވިފައި ހުންނަ ގަނޑު ތަކެއް ކުންފުނި ފެންނަންވާނެ. (ށ) ފަރާތްތަކުގެ ކުންފުނީ ބަދަލުކުރެވިފައި ހުންނަ ގަނޑު ތަކެއް. (ނ) ފ. ގުޅުގެ 4 ގަނޑު ތަކުގައި ކުރިން ވަޒަންދާ ގައުމީ ބޭންކުގެ ލައިސަންސް ހުންނަ ގަނޑު ތަކެއް.
·2·8	ވިލާ ކުރަންދާ ގަނޑު ތަކުގެ ތަފާސީލު ހުށަހަޅާ ފަރާތްތަކުން ހުށަހަޅާ ލިޔުންތަކުގައި ދައްކާ ގަނޑު ތަކުގެ ތަފާސީލު ހުށަހަޅަންވާނެ. ތަނާ ބެހޭ ލިޔުންތަކުގައި ދައްކާ ގަނޑު ތަކުގެ ތަފާސީލު ހުށަހަޅަންވާނެ. (ހ) ވިލާ ގަނޑު ތަކެއް (ށ) ތަރުޖަމާ ކުރެވިފައި ހުންނަ ގަނޑު ތަކެއް (ނ) ކުރަންދާ ގަނޑު ތަކެއް
·2·9	ފަރާތްތަކުގެ ހަނދާން ކުރެވޭ ގަނޑު ތަކުގައި ދައްކާ ގަނޑު ތަކުގެ ތަފާސީލު ހުށަހަޅާ ފަރާތްތަކުން ކުންފުނީ ލެޓަރ ހެޑްގައި ލިޔުންތަކުގައި ދައްކާ ގަނޑު ތަކުގެ ތަފާސީލު ހުށަހަޅަންވާނެ. ތަނާ ބެހޭ ތަފާސީލު ހުށަހަޅާ ފަރާތްތަކުން ވިލާ ހުށަހަޅާ ފަރާތްތަކުގެ ކުންފުނީ ކުރިއަށް ގެންދާ ގަނޑު ތަކެއް ހުންނަ ކަމަށް ބަލައި ދެވޭ ތަފާސީލު ހުށަހަޅަންވާނެ.
·2·10	ކުރަންދާ ވިލާ ގަނޑު ތަކުގެ ވެލިޑިޓީ ދުވަސް 90 (ދުވަހުގެ) ދިގުކަމުގައި ހުންނަންވާނެ.
·2·11	ފަރާތްތަކުން ހުށަހަޅާ ގަނޑު ތަކުގެ ބަޔާންކުރެވިފައި ހުންނަ ގަނޑު ތަކުގެ ތަފާސީލު ލިޔުމުގައި، ގަނޑު ދަރަޖަ ފުރިހަމަ ކުރެވިފައި ހުންނަންވާނެ.
·2·12	ފ. ގުޅުގެ ގަނޑު ބަލައިގަތުމުގެ ގޮތުގައި ގަނޑު ފ. ގުޅުގެ 6·3 ގައި ބުނެފައި ހުންނަ ގޮތަށް ހިނގަންވާނެ.
·2·13	ވިލާ ބާރުވެރިކުރެވިފައި ހުންނަ ބަޔަކަށް ވިލާ ހުށަހަޅަންވާނެ.
·2·14	ވިލާ ބާރުވެރިކުރާ ގަނޑު ތަކުގައި ބައްދަލުކުރާ ގަނޑު ތަކުގެ ތަފާސީލާ ގުޅިގެން ވިލާ ހުށަހަޅާ ފަރާތްތަކުން ބާރުވެރިކުރާ ގަނޑު ތަކުގެ ތަފާސީލު ހުށަހަޅަންވާނެ. ތަނާ ބެހޭ ވިލާ ހުށަހަޅާ ފަރާތްތަކުން ބާރުވެރިކުރާ ގަނޑު ތަކުގެ ތަފާސީލު ހުށަހަޅަންވާނެ.

	ކާރިއްޔާ ދާއިރާގެ ތެރެއިން ގެނައުން ހުށަހަޅާ ފަރާތްތަކުން ކަނޑައަޅާ ގަނޑަށް 5 (ފަސް) ދުވަހުގެ ތެރޭގައި ދެއްކުމަށް ވަޢުދުވުން.
2.15·	ކަނޑައަޅާފައި ވެއްޖެ ގަނޑުގެ ތެރެއިން ކަނޑައަޅާ ބައިކަން ހާސިލުކުރުމަށް ގެނައުން.
2.16·	ހުށަހެޅުމުގެ ދަށުގައި ދައްކަންޏާ ހަދިޔާ ފައިސާ ދެއްކުމުގެ ތެރޭގައި ގަބޫލުކުރާ 6 ގޮތް ބަޔާންކުރުން.

3· ކުރިއަށްގެންދާ ހިދުމަތްތަކާ ބެހޭ	
3.1·	ދެއްވާ ހިދުމަތްތަކާ ގުޅިގެން ހާސިލުކުރާ ފައިސާ ދެއްވާ ގޮތް ބަޔާންކުރުން.
3.2·	ތިމާވެއްޔާ ތަކެއްޗާ ގުޅިގެން ކަނޑައަޅާފައި ހުންނަ ގަޑިއިރުގެ ތެރެއިން 24 ގަޑިއިރު، ކުރިއަރުވާ ގޮތް ތަކެއް ދިނުމުގެ ގޮތުގައި ހާސިލުކުރާ ގޮތް ބަޔާންކުރުން.
3.3·	ފަރާތް ދެކެވޭ، ކާބޯ ފާޓަށް ބަދަލުގައި ކުރިއަށް ގެންދާ ހިދުމަތްތަކާ ގުޅިގެން ބަޔާންކުރުން.
3.4·	ތަކެއްގެ ސްޕެސިފިކޭޝަން ނުވަތަ ބަދަލުގައި ދޫކުރާ ތަކެއްގެ ތަފާތުތަކާ ގުޅިގެން ބަޔާންކުރުން.

ދަތުރުކުރާ ފަރާތުގެ ތަފްޞީލު

ދާއިރާގެ ހިންގުމާ ގުޅޭ ތަކެތި ހޯދުމުގެ ކޮމިޓީ ތަރުތީބުގައި ކުރިއަށް ގެންދާ ކަންތައް ކަށަވަރުކުރުމަށް ދަތުރުކުރާ ފަރާތުގެ ކުރިން ހުށަހަޅާ ލިޔުންތައް ބަލައި ބަލާ ފަރާތުގެ ތަފްޞީލު ހުށަހަޅާ ލިޔުން.

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

The deliverables of the cyber security consultancy provider include:

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

5. Overall Cyber Security Strategy and Work Plan: Developing a comprehensive strategy and work plan to address the organization's cybersecurity needs and objectives.
6. 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.
7. 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.
8. 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.
9. Incident Response Planning and Support: Developing incident response plans and providing support to the organization in responding to cybersecurity incidents effectively.
10. 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.
11. Security Architecture Review: Conducting reviews of the organization's security architecture to identify potential vulnerabilities and recommending appropriate measures to enhance security.
12. 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.
13. 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.
14. Vulnerability Management: Identifying and prioritizing vulnerabilities in the organization's systems and networks and recommending appropriate measures to mitigate risks.
15. Forensic Investigations: Conducting forensic investigations to identify the root cause of cybersecurity incidents and to gather evidence for legal proceedings if necessary.

16. Cloud Security Assessment and Advisory Services: Assessing the security of the organization's cloud-based systems and providing recommendations for enhancing security.
17. Physical Security Assessment: Assessing the physical security of the organization's facilities to identify potential vulnerabilities and recommending appropriate measures to enhance security.
18. 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.
19. 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.
20. 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. ޚިދުމަށް ހުށަހަޅާ ފަރާތުގެ ފަރާތާ ގުޅިގެން ބަލައިގަތުމަށް ހުށަހަޅާ ލިޔުންތައް.	
4.1.	ހުށަހަޅާ ފަރާތުގެ ނަން
4.2.	ޚިދުމަށް ހުށަހަޅާ ފަރާތް
4.3.	ގަވާއިދުގެ ދަށުން ލިބޭ ނަންބަރު / ތަކެއް ނަމަ ލިބޭ ނަންބަރު
4.4.	ތިރީގައިވާ ގޮތަށް ކުންފުނި / ފަރާތް ރަޖިސްޓަރ ކުރެވިފައިވާ ލިޔުންތައް. (ކުންފުނި / ފަރާތުގެ ނަން / ކުންފުނި / ފަރާތް ރަޖިސްޓަރ ކުރެވިފައިވާ ގޮތާ ގުޅިގެން ލިޔުންތައް)
4.5.	ފިޔަވަޅު ކުރެވިފައިވާ ކުންފުނި ފަރާތްތަކުގެ ލިސްޓެއް ހުށަހަޅަންވާނެ.
4.6.	ފިޔަވަޅު ކުރެވިފައިވާ ކުންފުނި ފަރާތްތަކުގެ ނަން ތަފާތު ގޮތްގޮތަށް ހުށަހަޅަންވާނަމަ، ތަފާތު ގޮތްގޮތަށް ހުށަހަޅާ ލިޔުންތައް (ތ.ގދ. ދ. ތަކެއް) - ލިޔުންތަކުގެ ގަޑިތަކުގެ ތަފާތު
4.7.	ފަށާ ދުވަހުގެ ތެރޭގައި ހުށަހަޅާ ލިޔުންތަކުގެ ކޮޕީ ހުށަހަޅާ ފަރާތުގެ ސޮއި ލިބިގެންވާ ލިޔުންތައް
4.8.	ފަށާ ދުވަހުގެ ތެރޭގައި ހުށަހަޅާ ލިޔުންތަކުގެ ކޮޕީ ލިބިގެންވާ ލިޔުންތައް (ކ.ގދ. ކުރިއަށް ލިބޭ ނަންބަރު)
4.9.	ފަށާ ދުވަހުގެ ތެރޭގައި ހުށަހަޅާ ލިޔުންތަކުގެ ކޮޕީ ކުންފުނީ ސަރުކާރުން ދޫކުރެވިފައިވާ ކުންފުނި ރަޖިސްޓަރ (ކުންފުނި ގަވާއިދު 03 ގެ ދަށުން)
4.10.	ދަށުން ބަލައި ގެންދާ ކުންފުނި ފަރާތްތަކުގެ ލިސްޓެއް
4.11.	ފާރު ކުޑަ "ގަވާއިދުގެ ދަށުން ލިބޭ ކުންފުނި ފަރާތް" ތަކުގެ ލިސްޓެއް ހުށަހަޅާ ދުވަހުގެ ކުރިން ފަސް ބަސްގެ ތެރޭގައި ކުންފުނި ރަޖިސްޓަރ ކުރެވިފައިވާ ގޮތާ ގުޅިގެން ލިޔުންތައް، 2019 ، 2020 ތަކުގެ 2021 ވަނަ ދުވަހާ ގުޅިގެން ގަވާއިދުގެ ދަށުން ލިބޭ ނަންބަރު ލިޔުންތައް (ދަށުވަނަ 03 ގެ ދަށުން 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 marks will be awarded for each reference document submitted that meets the following requirements. The maximum score for this section is 35 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. ތަކެއްގައި ހިމަނަންޖެހޭ ކޮންޓެންޓް

- ލިޔުންތަކުގައި ބޭނުންކުރާ ބަހަކީ ދިވެހި ބަހެއް ނުވާނަމަ ދިވެހި ބަހަށް ތަރުޖަމާ ކުރެވިފައި ހުރުން.
- ލިޔުންތަކުގައި ހިމަނާ ހުރި ތަކެއްޗާ ގުޅޭ ތަފާތު ތަކެއްޗާ ގުޅުވައިގެން ބަލައި ގެންނަން ޖެހޭ ކަންކަން ހުރުން.
- ފާރާ ދުވަސްތަކުގައި ތަކެއްޗާ ގުޅޭ ތަފާތު ތަކެއްޗާ ގުޅުވައިގެން ބަލައި ގެންނަން ޖެހޭ ކަންކަން ހުރުން. 2019، 2020 ، 2021 ވަނަ އަހަރުގެ ފާރާ ދުވަސްތަކުގައި ތަކެއްޗާ ގުޅޭ ތަފާތު ތަކެއްޗާ ގުޅުވައިގެން ބަލައި ގެންނަން ޖެހޭ ކަންކަން ހުރުން.
- ތަކެއްގައި ހިމަނާ ހުރި ތަކެއްޗާ ގުޅޭ ތަފާތު ތަކެއްޗާ ގުޅުވައިގެން ބަލައި ގެންނަން ޖެހޭ ކަންކަން ހުރުން. ލިޔުންތަކުގައި ބޭނުންކުރާ ބަހަކީ ދިވެހި ބަހެއް ނުވާނަމަ ދިވެހި ބަހަށް ތަރުޖަމާ ކުރެވިފައި ހުރުން.

6.1. ލަނޑުދަނޑި ބަދަލުގެ ބޭނުންވާ ތަކެތި

National Centre for Information Technology

ދާއިރާގެ ގޮތުގައި ފުރިހަމަ ކުރަންވާ ތަކެތި

#	ލަނޑުދަނޑި ތަފްޞީލު	ޔުނިޓް	ފުރަތަ
1	ލަނޑުދަނޑި ބަދަލުގެ ބޭނުންވާ ތަކެތި		
2	ޕްރޮގްރާމް ލަނޑުދަނޑުވުން		
3	ކުރިއަށްގޮސް ބައެއް ދުވަސް / ގަޑި ދުވަހުގެ ތެދުވުން ކަށަވަރުކުރުން		
4	ތިލަފުށީގައި ބަދަލުކުރެވޭ ކުލަތަކާ ވިދާލައިގަނެ ދިނުން. (ކާނާ / ފާރުގައި / ކައިރިއަށް ދާ ބަސްތަކާ / ތަކެތި ގެންނަ ގޮތް)		
5	ދިރިއުޅޭ ތަނާ ބައްދަލުވެ ލިޔުންތަކުގެ ވިދާލައިގަނެ ކަށަވަރުކުރުން.		
6	ދިރިއުޅޭ ތަނާ ބައްދަލުވެ ލިޔުންތަކުގައި ކުރިން ބަދަލު ކުރި ގޮތް ވިދާލައިގަނެ ލިޔުންތަކުގައި ބަދަލުކުރެވޭ ތިލަފުށީ ވިދާލައިގަނެ (ލަނޑުދަނޑި ބަލައި ބަލައި ބަދަލުކުރުން) – ބަދަލުކުރެވޭ ގޮތުގައި		
7	ލަންޑިގުޅި ބައްދަލުވުން ބޭއްކުރުމާ ގުޅިގެން ދަންނަ ބަދަލުކުރެވޭ ތަކެތި ހޯދުން ހިނގާ ގޮތް		
8	ލަންޑިގުޅި ބައްދަލުވުން ބޭއްކުރުމާ ގުޅިގެން ދަންނަ ބަދަލުކުރެވޭ ފެށުންތައް (ފެށުން.ދިވެހި ބަދަލުކުރެވޭ ގޮތް)		
9	ލަންޑިގުޅި ބައްދަލުވުން ބޭއްކުރުމާ ގުޅިގެން ކުރަންޖެހޭ ތަކެތި ތިރީގައި ލިޔެދޭ (ދުވަސް 03 ކުރިން ހުށަހެޅުން)		
10	ކަނޑުވަޅުގެ ތަފާތު ބަދަލުތަކާ ގުޅިގެން ދަނޑުވެރިންގެ ކަންތައް ބަލައި ގަތުމާ ދުވަސް ދުވަހުގެ ތަފްޞީލު		
11	ފާރ ފުރަތަ ދުވަސްތަކުގައި ސާވޭކުރާ ދަނޑުވެރިންގެ ކަންތައް ކަށަވަރުކުރުމަށް "ކުރިއަށްގޮސް ތެދުވުން" ގަބޫލުކުރާ ދަނޑުވެރިންގެ ބަދަލުތަކާ ގުޅިގެން ކުރިއަށް ގެންދާ ކަންތައް (2019 ، 2020 ގެ 2021 ވަނަ ބަލައި ކުރިއަށްގޮސް ކަށަވަރުކުރާ ގޮތް) ތިލަފުށީގައި ދުވަހުގެ ގަޑި ކަނޑައަޅާ ގޮތް (ދުވަހުގެ 03 ގެ ކުރިން 03)		

6.2 ސ.ތަކުން ހުށަހެޅުން

National Centre for Information Technology

ދާއިރާގެ ގޮތުގައި ކުރިއަށް ގެންދާ ތަރައްޤީ ޕްރޮގްރާމް ހ.ބ.ދ.ކ

ތަކުލީފުގެ ނަންބަރު:		ގޮތުގެ:	
ސ.ތަކުގެ ގުޅުންހުރި ކަންތައްތަކުގެ ތަފްޞީލު ހުށަހަޅާ ފަރާތުގެ ކަންތައް			
ސަބަބު:			
ތަކުލީފު ދިނުމުގެ ތަރުތީބު:			
ހަމަ ނިންމާ ތާރީޚު:			
ގޮތުގެ:			
ސ.ތަ:			
ތ ސ.ތަކުގެ ހުށަހެޅުމާ ގުޅިގެން ކަންތައް ކުރުމަށް ކަނޑައަޅާ ތާރީޚުގެ ކުރިން ތ ސ.ތަ ކުރިއަށް ގެންދާ ފަރާތުގެ ކަންތައް. ތ ސ.ތަ ކުރިއަށް ގެންދާ ފަރާތުގެ ކަންތައް ކުރުމަށް ކަނޑައަޅާ ތާރީޚުގެ ކުރިން ސ.ތަ ކުރިއަށް ގެންދާ ފަރާތުގެ ކަންތައް ކުރުމަށް ކަނޑައަޅާ ތާރީޚުގެ ކުރިން			
ސ.ތަކުން ލިބޭ ފައިދާ (ތ ސ.ތަ ކުރިއަށް ގެންދާ ފަރާތުގެ ކަންތައް، ކުރިއަށް ގެންދާ ކަންތައް ދެމެހެއްޓުމުގެ ކަންތައް، ސ.ތަ ކުރިއަށް ގެންދާ ފަރާތުގެ ކަންތައް)			
ސަބަބު:		ތ ސ.ތަ ކުރިއަށް ގެންދާ ފަރާތުގެ ސ.ތ.ކ	
ތަކުލީފު ދިނުމުގެ ތަރުތީބު:			
ހަމަ ނިންމާ ތާރީޚު:			
ގޮތުގެ:			
ސ.ތަ:			

6.2. ފައިނޭންޝަލް ޕްރޮޕޯސަލް ފޯމް (ޖެން ފޯމް-1) ނަމޫނާ ފޯމުގައި ބަޔާންކުރާ މަޢުލޫމާތު ހިމެނޭ ކޯޓޭޝަން. މި ފޯމް ނަމޫނާ ކޯޓޭޝަނާއި އެކު ހުށަހަޅަންވާނެއެވެ. މި ފޯމުގެ ހުރިހާ މަޢުލޫމާތެއް ފުރަންވާނެއެވެ. ނަމޫނާ ކޯޓޭޝަންގައި ހިމަނަންވާނެއެވެ.

بسم الله الرحمن الرحيم

National Centre for Information Technology

ނޭޝަނަލް ސެންޓަރ ފޯރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ

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 ފަރާތުގެ ފަސް (2-ފުރާ) ހަ

National Centre for Information Technology

ދާއިރާގެ ފަރާތުން ހިންގާ ފަރާތް

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 ފަރާތުން ހުށަހެޅި ހުށަހެޅުން ސަލާމަތްވާ ތާރީޚް

[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. އެއްބަސްވުމުގެ ނަމޫނާ

އެއްބަސްވުން

ނަންބަރު:

1. ތަޢާރަފު.

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

2. އެއްބަސްވުމުގެ ބައިވެރިން.

2.1. މި އެއްބަސްވުމުގައި މަސައްކަތް ހަވާލުކުރި ފަރާތްތަކުގައި ބައިވެރިވެފައިވަނީ، ނޭޝަނަލް ސެންޓަރ ފޯރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީއެވެ.

2.2. މަސައްކަތާއި ހަވާލުވާ ފަރާތް ކަމަށް ބައިވެރިވެފައިވަނީ (ކުންފުނި ނުވަތަ ވިޔަފާރިގެ ނަން)

3. އެއްބަސްވުމުގައި ހިމެނޭ ތަކެއްޗާއި މަސައްކަތްތައް

3.1. މަސައްކަތް ހަވާލުކުރި ފަރާތުން (ތާރީޚް) ވަނަދުވަހު ކުރި އިޢުލާން (ނަންބަރު) އާއި ގުޅިގެން މަސައްކަތާއި ހަވާލުވި ފަރާތުން ހުށަހަޅާފައިވާ، (މި އެއްބަސްވުމުގެ ޖަދުވަލު 1 ގައި އެއްކަރުދާސްކުރެވިފައިވާ) ޕްރޮޕޯސަލްގައިވާ ތަކެތި/މަސައްކަތް ހަވާލުކުރިފަރާތަށް ސަޕްލައިކޮށްދިނުން.

4. މަސައްކަތުގެ އަގު.

4.1. ޖަދުވަލު 1 ގައިވާ މަސައްކަތްތައް ކުރުމަށް މަސައްކަތުގެ އަގު ޖުމްލަގައި ކަނޑައަޅާފައިވަނީ (އަގު) އެވެ.

5. މަސައްކަތުގެ މުއްދަތު.

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

(ހ) އެއްބަސްވުމުގައި ސޮއި ކުރާ (ތާރީޚް) އެވެ.

(ށ) އެއްބަސްވުމުގައިވާ މަސައްކަތް ނިންމަންޖެހޭ (ތާރީޚް) އެވެ.

6. މަސައްކަތަށް ފައިސާދެއްކުން

6.1. މަސައްކަތް އެއްބަސްވުމާއި ފުރިހަމަޔަށް ނިންމުނުކަމަށް މަސައްކަތް ހަވާލުކުރިފަރާތުން ނިންމުމުން، މަސައްކަތް ހަވާލުވިފަރާތުން މަސައްކަތުގެ ބިލުގެ އަސްލު، މަސައްކަތް ހަވާލުކުރި އޮފީހުގެ ރަސްމީ އީމެއިލް ނުވަތަ ރިސެޕްޝަނަށް ހުށަހަޅަންވާނެއެވެ. އަދި މި ބިލަށްވާ ފައިސާ 30 (ތިރީސް) ދުވަހުގެ ތެރޭގައި ހަވާލުކޮށް ނިންމަންވާނެއެވެ.

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 ތަނަވަސް ފެންވަރެއްގައި މަސައްކަތް ނިންމުމަށްފަހު މަސައްކަތް ޙަވާލުކުރި ފަރާތާ ޙަވާލު ކުރަންވާނެއެވެ.

8. މަސައްކަތަށް ބަދަލުގެނައުން.

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

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

(ށ) ސްކޯޕް ކުރުރުގައިވާ ކަންކުރަން، މަސައްކަތް ކުރާ ފަރާތުން އެކަމަށް ހިނގާނެ ޚަރަދު ބަޔާންކޮށް ލިޔުމުން މަސައްކަތް ޙަވާލުކުރި ފަރާތަށް ހުށަހަޅަންވާނެއެވެ.

(ނ) މިގޮތުން އިތުރުކުރާ މަސައްކަތެއް ފަށަންވާނީ ދެފަރާތުން އެއްބަސްވުމެއް ހަދައި އެއްބަސްވުމުގައި ސޮއިކުރުމަށްފަހުއެވެ.

(ރ) އަގަށް އެއްބަސް ނުވެވޭ ހާލަތްތަކުގައި އެހެން ފަރާތަކާއި އެކު މަސައްކަތުގެ އެއްބަސްވުން ހުއްޓުވުމުގެ އިޚްތިޔާރު، މަސައްކަތް ޙަވާލުކުރާ ފަރާތަށް ލިބިގެންވެއެވެ.

(ބ) ކަނޑައެޅިފައިވާ މުއްދަތަށް މަސައްކަތް ނިންމުމަށް މަސައްކަތް ހަވާލުވިފަރާތަށް ދަތިވާނަމަ ސަބަބު ބަޔާންކޮށް މަސައްކަތް ހަވާލުކުރިފަރާތުން ބަޔާންކުރާ ހުއްޓުމާއި ދުރާލައި ލިޔުމުން އަންގަންވާނެއެވެ.

8.2. ލިޔުމުން ހުށަހަ ތަފާތުތަކާ ގުޅޭ ކަންކަމުގައި ކޮންމެ ދުވަހެއްގެ 10:55 ގަޑިއަށް ފަހު ހުށަހެޅުނު ލިޔުންތައް ދެން ބަލައިގަނެ ނުވާނެ.

8.3. ލިޔުން ހުށަހެޅުނު ފަރާތުގެ ސޮއި ލިޔުމުގައި ހުންނަންވާނެ.

9. ކަނޑައެޅިފައިވާ ދުވަސްތަކުގެ ތެރެއިން ދަށ ކުރުން.

9.1. ލިޔުމުން ފާސްކޮށްދީފައިވާ ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ކަނޑައެޅިފައިވާ ދުވަސްތަކުގެ ތެރެއިން ދަށ ކުރުމަށް ކަނޑައެޅިފައިވާ ދުވަސްތަކުގެ ތެރެއިން ދަށ ކުރުން.

9.2. ދެއްވާފައި ހުންނަ ކަނޑައެޅުމުގައި ކަނޑައެޅިފައިވާ ދުވަސްތަކުގެ ތެރެއިން ދަށ ކުރުމަށް ކުރިއަށް ގެންދާ ދުވަހުގެ 10:71 ގަހަ ފާޅުގައި ހުންނަ ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ކަނޑައެޅިފައިވާ ދުވަސްތަކުގެ ތެރެއިން ދަށ ކުރުން ކުރެވޭނެ ގޮތް ބަލައިގަންނަންވާނެ.

9.3. ދުވަހަކަށް -/5,000,000 ގަދަ ފަދަ ފައިސާ ކަނޑައެޅި، ދުވަހަކަށް 0.005 (ސަތޭކަ ބައިގެ ފަހެ) ގ ގުޅޭ ކަންކަމުގައި ދެ ކުރިން ކަނޑައެޅި ދުވަސްތަކުގެ ތެރެއިން ދަށ ކުރެވޭ ގޮތް

ދަށ ކުރެވޭ ދުވަސްތަކުގެ ތެރެ = CP*0.005*LD

ކަނޑައެޅި ދުވަހަކަށް -/5,000,000 ގަދަ ފަދަ ފައިސާ ކަނޑައެޅިފައިވާ ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ދެ ކުރިން ކަނޑައެޅި ދުވަސްތަކުގެ ތެރެއިން ދަށ ކުރެވޭ ގޮތް ކަނޑައެޅިފައިވާ ދުވަސްތަކުގެ ތެރެ ދަށ ކުރެވޭ ގޮތް

ދަށ ކުރެވޭ ދުވަސްތަކުގެ ތެރެ = CP*0.0025*LD

CP (ކުރިން ކަނޑައެޅި ދުވަހުގެ ގަހަ): ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ދެ ކުރިން ކަނޑައެޅި ދުވަހުގެ ގަހަ

LD (ދުވަސް ތެރެއިން): ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ދެ ކުރިން ކަނޑައެޅި ދުވަސްތަކުގެ ތެރެ

9.4. • ލިޔުމުން ލިޔެ ހުށަހެޅުމުގައި ކަނޑައެޅި ގަސްދުގެ ތެރެއިން ކުރިއަށް ގެންދާ ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ކަނޑައެޅިފައިވާ ދުވަސްތަކުގެ ތެރެ (ގަބޫލުކުރާ ކަނޑައެޅި) ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ދަށ ކުރެވޭ ގޮތް ބަލައިގަންނަންވާނެ.

9.5. ކަނޑައެޅިފައި ހުންނަ ލިޔުމުގައި ކަނޑައެޅި ދުވަހުގެ ތެރެއިން ކޮންމެ ދުވަ ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި 15% (ފަސްދިހަ ސައިކަތު) ކަނޑައެޅި ދުވަހުގެ ތެރެ ދަށ ކުރެވޭ ގޮތް ބަލައިގަންނަންވާނެ.

9.6. ތިރީގައި ބަޔާންކޮށްފައިވާ ގޮތުގެ 15% (ފަސްދިހަ ސައިކަތު) ކަނޑައެޅި ދުވަހުގެ ތެރެ ދަށ ކުރެވޭ ގޮތް ކަނޑައެޅިފައިވާ ދުވަސްތަކުގެ ތެރެ ދަށ ކުރެވޭ ގޮތް، ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ކަނޑައެޅި ދުވަހުގެ ތެރެ ދަށ ކުރެވޭ ގޮތް ބަލައިގަންނަންވާނެ. ކަނޑައެޅި ތަކެއްޗާ ގުޅޭ ކަންކަމުގައި ކަނޑައެޅި ދުވަސްތަކުގެ ތެރެ

ގަބޫލުކުރުމުން ހިނގާ ކަންތައް ހުރަސް ކުރުމަށް ކުންފުނިން ފުރިހަމަ ކުރާ ކަންތައް ހިނގާ ގޮތް ބަލައި ގަބޫލުކުރުމަށް ކުންފުނިން ބާއްވާ ކޮމިޓީ ކަމަށް ވާނެ ކަމަށް ކަނޑައަޅަ ކޮމިޓީ ކަމަށް ވާނެ ކަމަށް ކަނޑައަޅަ

9.7. ތިރީ ބުރަކާރުގެ ކަންކަމުގައި ކުންފުނިން ކުރިއަށް ގެންދާ ބުރަކާރު ކަންކަމުގައި ކުންފުނިން ކުރިއަށް ގެންދާ

10. ބުރަކާރު ދެއްކުމުގެ ގޮތް 10.1. ތިރީގައި ބުރަކާރު ދެއްކުމުގެ ގޮތް ތިރީގައި ބުރަކާރު ދެއްކުމުގެ ގޮތް ކުންފުނިން ކުރިއަށް ގެންދާ ގޮތަށް ބުރަކާރު ދެއްކުމުގެ ގޮތް ކުންފުނިން ކުރިއަށް ގެންދާ ގޮތަށް ބުރަކާރު ދެއްކުމުގެ ގޮތް ކުންފުނިން ކުރިއަށް ގެންދާ ގޮތަށް ބުރަކާރު ދެއްކުމުގެ ގޮތް ކުންފުނިން ކުރިއަށް ގެންދާ ގޮތަށް

11. ދިގުދާ ގަތްކަމުގެ ކަންކަން ދިގުދާ ގަތްކަމުގެ ކަންކަން ދިގުދާ ގަތްކަމުގެ ކަންކަން ދިގުދާ ގަތްކަމުގެ ކަންކަން 11.1. ކުންފުނިން ކުރިއަށް ގެންދާ ދާއިރާގެ ތެރެއިން ދިގުދާ ގަތްކަމުގެ ކަންކަން ދިގުދާ ގަތްކަމުގެ ކަންކަން ދިގުދާ ގަތްކަމުގެ ކަންކަން ދިގުދާ ގަތްކަމުގެ ކަންކަން ކުންފުނިން ކުރިއަށް ގެންދާ ދާއިރާގެ ތެރެއިން ދިގުދާ ގަތްކަމުގެ ކަންކަން ދިގުދާ ގަތްކަމުގެ ކަންކަން ދިގުދާ ގަތްކަމުގެ ކަންކަން ދިގުދާ ގަތްކަމުގެ ކަންކަން

12. ދެމަދުވެގެންވާ ކަންކަން. 12.1. ތިރީ ބުރަކާރު ކުރިއަށް ގެންދާ ގޮތުގެ ދެމަދުވެގެންވާ ކަންކަން ތިރީގައި ބުރަކާރު ކުރިއަށް ގެންދާ ގޮތުގެ ދެމަދުވެގެންވާ ކަންކަން ތިރީގައި ބުރަކާރު ކުރިއަށް ގެންދާ ގޮތުގެ ދެމަދުވެގެންވާ ކަންކަން ތިރީގައި ބުރަކާރު ކުރިއަށް ގެންދާ ގޮތުގެ ދެމަދުވެގެންވާ ކަންކަން

ދަށުގައިވާ ބުރަކާރުގެ ކަންކަމުގެ ދަށުގައި ބުރަކާރު ކުރިއަށް ގެންދާ (ތިމާ) ނ (ތިމަން) ދުވަހުގެ ތެރެއިން ކުންފުނިން ކުރިއަށް ގެންދާ

ދަށުގައިވާ ކަންކަމުގެ ތަފްޞީލް	ދަށުގައިވާ ކަންކަމުގެ ތަފްޞީލް
(ދަށުގައިވާ ކަންކަމުގެ ތަފްޞީލް ކުންފުނިން ކުރިއަށް ގެންދާ ގޮތް)	**(ދަށުގައިވާ ކަންކަމުގެ ތަފްޞީލް ކުންފުނިން ކުރިއަށް ގެންދާ ގޮތް)**

ގަބޫލުކުރި ފަރާތުގެ ނަން : ގަބޫލުކުރި ފަރާތުގެ ނަން :

ދުވަސް : ދުވަސް :

ސޮއި: ދަށުގައިވާ ކަންކަމުގެ ތަފްޞީލް

ދަނޑުވަށް ހަލާކުވި ގޮތް	ދަނޑުވަށް ހަލާކުވި ގޮތް
ނަންބަ:	ނަންބަ:
ތަރިން:	ތަރިން :
ތާރީޚް :	ތާރީޚް :