INSTRUCTIONS TO TENDERERS FOR

The Provision of Computer Network Maintenance Services

to the Environmental Protection Department

ENVIRONMENTAL PROTECTION DEPARTMENT

INTRODUCTION

1. The purpose of the Instructions for Tenderers document is to identify a suitable agency (hereafter referred to as Consultant) to provide computer hardware maintenance and software services to the Environmental Protection Department, Ministry of Environment and National Beautification, Green and Blue Economy.

BACKGROUND

2. The Environmental Protection Department (hereafter referred to as the Department) is a government department within the Ministry of Environment and National Beautification, Green and Blue Economy. The Department is a regulatory agency which carries out a number of functions in the area of environmental management which includes ambient air quality and water quality management.

STATEMENT OF WORK

3. The Consultant would be required to carry out the following services on the equipment listed below and any equipment installed in place there of:

Hardware Services

i. Reconfigure (if necessary) and maintain the multiple server computer network inclusive of the firewall, antivirus and network backup systems;
ii. Develop, maintain and update security for the entire computer network system including antivirus, antispyware, user permissions and application access and produce security logs;
iii. Provide backup systems in accordance with the network Back-up Policy of the Department (See Appendix C);
iv. Set-up and implement server operations and network devices including user management, file management, network security, monitoring and services updates for all server services with the approval of the Director;
v. Provide network maintenance and quarterly hardware and software maintenance for all computer systems and network devices listed in Appendix B, which should include software and hardware checks, profiles clean-ups, motherboard maintenance and servicing to prevent corrosion and maintain efficiency of the computer systems;
vi. To develop and manage the server disaster recovery system;
vii. Provide emergency maintenance in response to faults or malfunction of equipment and software or malicious damage;
viii. Repair hardware and software damage to equipment;

ix. Replace parts and install batteries necessary for the proper functioning of the equipment;
x. Conduct other hardware and software services which may include the installation of additional computer systems and software updates;
xi. Provide computer server awareness training;
xii. Provide end user and mapping support services for all devices;
xiii. Any other approved services by the Director to ensure minimum downtime of the Computer Network.

Software Services

i. Installation of software and related updates and re-installation as required;
ii. Provision of software support for programmes;
iii. Provision of basic training in the use of installed software;
iv. Set up and maintain security of the information on the servers and produce monthly reports on the system including security breaches, adequacy of operation and any other critical information required to assess performance and ensure the security of information;
v. Provision of on-site and off-site back up of the data on the server;
vi. Provision of technical support in the event of system errors or failures;
vii. Ensure all critical software license are up-to-date inclusive of Microsoft products, firewall, antivirus, server operating systems.

DURATION

4. The successful Consultant will be awarded a fixed contract for a period of two (2) years commencing April 1, 2023 and concluding March 31, 2025.

SCOPE OF SERVICES

5. The computer hardware and software maintenance services are to be performed between the hours of 8:30 a.m. and 4:30 p.m. at the Environmental Protection Department. However, where services can be performed remotely the Consultant is encouraged to do so but these should be itemised in the "approach section" of the proposal.

6. The Consultant shall prepare a report detailing the quarterly hardware and software maintenance services provided which should be submitted to the Director of the Department. This would be the basis for the quarterly disbursement.

7. The Consultant shall report monthly to the Director of the Department in an agreed format on the security threats to the servers and indicate preventative and remediation methods to address any challenges.

APPLICATION PROCEDURE

8. Prospective tenderers will be invited to attend a meeting on Friday September 23, 2022 at Conference Room, Environmental Protection Department, **L.V. Harcourt Lewis Building, Dalkeith, St. Michael** commencing at **10:00 a.m.** to discuss any concerns with the invitation for tender.

9. Subsequent to the meeting with prospective tenderers, the period allocated for the preparation and submission of tenders is twenty-one (21) days.

SELECTION CRITERIA

10. The Tenders will be assessed using the criteria outlined in Table 1.

Table 1: Tender assessment criteria.

CRITERION	DESCRIPTION	MEASURE	MAXIMUM SCORE	WEIGHTING
Experience	The number of years of experience providing similar services.	The number of years of experience in the field.	10	10
	The proven record of the company with provision of similar services.	List of similar contracts awarded within the past five years.	10	10
Key Personnel	The suitability of the qualifications of the key personnel who would be assigned to carry out the services.	Qualifications of key personnel.	15	20
	The availability of adequate resources to successfully carry out the services required.	Resources identified to provide services.	15	15

CRITERION	DESCRIPTION	MEASURE	MAXIMUM SCORE	WEIGHTING
Approach to Server Management and Maintenance	Methodology proposed to ensure continuous management, maintenance and protection of the network system.	The demonstrated proven record of the company. A proposed schedule for quarterly computer hardware maintenance and software maintenance.	10	20
Cost	The cost for the provision of services.	The cost of the tender.	15	25

11. The conforming tender with the highest score will be selected.

12. The Department reserves the right to accept or reject any tender and to reject all tenders.

TENDER SUBMISSION AND FORMAT

13. Candidates should submit the completed Form of Tender along with one (1) hard copy of the tender in the format provided in the following paragraph. Tenders should be delivered, in a sealed envelope labelled with the subject given below, to the address below no later than 4:30 p.m. on Friday October 14, 2022.

Director
Environmental Protection Department
L. V. Harcourt Lewis Building
Dalkeith
St. Michael

Subject: Invitation to Tender for the Provision of Computer Network Maintenance Services to Environmental Protection Department

14. The tenders should follow the format provided below and should be no more than twenty-five (25) pages, excluding appendices.
    i. *Company Background*

This section should contain a brief overview of the business and clearly identify the number of years of operation of the business. A copy of the certificate of incorporation or business registration certificate should also be included in the submission.

ii. *List of Key Personnel and their Qualifications*
This section should identify the key personnel that will be assigned to perform the hardware and software maintenance, as well as all of their **relevant** qualifications e.g. degrees, diplomas, certificates and professional designations.

iii. *List of Similar Contracts*
List similar contracts awarded within the last five years and current contact information for the organizations where contract services were provided.

iv. *Approach to Server Management and Maintenance*
Provide a detailed explanation on how server operations will be implemented including user management, file management, network security, system back-ups and monitoring for all server services. The proposed schedule for quarterly computer hardware maintenance and software maintenance shall also be provided.

v. *Proposed Cost*
Specifies the overall cost to perform the services and a breakdown of cost in relation to the activities outlined in the statement of work. The costs shall be itemised giving details for salaries, and reimbursables on an annual basis. . The quote for the services should be set out in the two financial years of the Contract period.

15. The Form of Tender at Appendix A must be completed and submitted with tender.

PAYMENT

16. Payment will be made quarterly to the successful Consultant by the Environmental Protection Department, Ministry of Environment and National Beautification, Green and Blue Economy over the duration of the Contract

TERMS AND CONDITIONS

17. The proposed contract for the provision of services is included in Appendix D.

APPENDIX A:

Form of Tender

FORM OF TENDER

TO: The Director
Environmental Protection Department
Ministry of Environment and National Beautification, Green and Blue Economy
L V Harcourt Lewis Building
Dalkeith
ST. MICHAEL

Tender for the Provision of Computer Network Maintenance Services

Having read and understood the relevant Tender Notice and Instructions to Tenderers and having also obtained further particulars from the Environmental Protection Department, Ministry of Environment and National Beautification, Green and Blue Economy, I/we hereby offer to supply the services tendered for in the attached Proposal at the price stated in said Proposal.

2. I/We undertake, if our tender is accepted, to satisfy the requirements of the Environmental Protection Department and guarantee to supply the services on a quarterly basis over the two-year period 2023 to 2025 at such times as agreed by the Environmental Protection Department.

3. I/We agree that all deliveries shall be at our expense.

4. I/We agree to comply with the conditions set out in the Tender Notice, specifications and Instructions to Tenderers.

5. I/We agree to abide by this Tender for the period of ninety (90) calendar days from the date fixed for receiving the same and it shall remain binding upon me/us and may be accepted at any time before the expiration of that period.

6. Unless, and until a written Agreement is prepared and executed, this Tender together with written notification of award and our acceptance thereof shall constitute a binding contract between us and the Government of Barbados.

7. I/We understand that the Government is not bound to accept the lowest or any Tender.

Name of Tenderer: .....

Address: .....

.....

Telephone No.: .....

Email Address: .....

Signature: .....

Date: .....

APPENDIX B:

Equipment List

TYPE OF EQUIPMENT	NUMBER
Desktop Computers	34
Laptops	8
Tablets	8
Printers	3
Multifunction Printer/Scanner/Copier	2
Servers	2
Switches	2
Routers	2
Firewall	1

APPENDIX C:

Environmental Protection Department's
Network Server Back-up Policy

1 OVERVIEW

Background

The Environmental Protection Department collects and generates significant volumes of environmental data, reference materials and technical documents, which are stored electronically. The availability of this data is crucial to the operations of the Department.

In order to minimize any potential loss or corruption of this data, the data must be backed-up adequately. Adequate backups will allow data to be safely stored and be readily recovered as necessary. This can only occur if there is a clear policy and strategy to manage the process of backing-up and safeguarding critical information.

Purpose

The purpose of this strategy is to:

- Safeguard the electronic data and resources of the Environmental Protection Department (EPD).
- Prevent the loss of data if and when hazard events occur. These events can include:
  - ⇒ accidental deletion;
  - ⇒ virus attack;
  - ⇒ theft;
  - ⇒ corruption of data;
  - ⇒ system failure;
  - ⇒ power surge; or
  - ⇒ disaster.
- Permit timely restoration of information and business processes with minimum effort, cost or data loss.
- Manage and secure backup and restoration processes and the media employed in the process.

Scope

This strategy applies to all the servers of the EPD and does not apply to the information on individual computers within the Department.

The retention periods of information contained within system level and offsite backups are designed for recoverability of information up to **one week** prior to a catastrophic system failure. *Other forms of backup allow for recoverability up to two months prior to the failure*.

The system backups are not meant for the following purposes:

- Saving data indefinitely.
- Maintaining a chronicle of backed-up data.

2 STRATEGY

Features

The data protection strategy for the EPD addresses five areas that are deemed critical for safeguarding the Department's electronic data. These areas are:

- Maintaining a reliable power supply
- Mitigating the impact of hardware faults
- Virus and firewall protection
- Contracting an ICT service provider
- Effective backing-up of data including:
    - Onsite backup
    - Offsite backup
    - A backup management procedure

Additionally, the policy specifies the responsibilities of the various parties involved in the data protection process.

Guide Lines

Power Supply

A Departmental server must be insulated from variations in the public power supply and be able to continue operation in the event of a power outage until it can be shutdown safely.

Consequently, the server must be connected, **at all times**, to a suitable device (or devices) that offers:

- voltage regulation in order to provide protection against power surges and during low voltage conditions; and
- uninterruptable power supply.

Additionally, the batteries on the device should be changed every three years or as necessary.

Furthermore, the power requirements of the server and its associated equipment must not exceed 80% of the rated capacity of the device.

Mitigation of the impacts of server hardware faults

In order to quickly recover from hardware faults such as damaged hard drives, the server must utilize RAID. RAID stands for Redundant Array of Inexpensive/Independent Disks. In general, a RAID-enabled system uses two or more hard disks to improve the performance or provide some level of fault tolerance for the server. Fault tolerance means that in the event of hard drive failure, the server can still operate. Fault tolerance lessens interruptions in productivity and also decreases the chance of data loss.

The levels of RAID suitable to the Department's server(s) are RAID 5, RAID 6 or RAID 10. These offer increased fault tolerance and system performance.

Virus and Firewall Protection

The server must have antivirus software installed. The software should offer:

- *Real-time Scanning:* The software should monitor network data as it is coming into the computer to intercept any malware as it enters the system.
- *On-access Scanning:* The software should scan files as they are opened or accessed to detect any malware.
- *On-Demand Scanning:* On-demand scanning provides the ability to perform a custom scan of a file, folder or drive initiated by the user.
- *Heuristic Scanner:* Heuristic scanning uses what is known about existing malware and what it has learned from past experience to identify new threats even before the antivirus vendor creates an update to detect it.
- *Compressed File Scanning:* Some malware may come inside a compressed file such as a ZIP file, or may be embedded in compressed files within compressed files. The antivirus software should be able to scan many levels (i.e. folders, executable files, documents or other compressed file) within a compressed file.
- *Scheduled Scans:* The software should provide some method of creating a schedule to set when the software will automatically perform a scan.

Additionally, the method should be flexible enough to allow users to run any type of pre-configured or custom scan at the scheduled time.

- *Script Blocking:* Script languages are frequently used to execute malicious code from web sites. The antivirus programme must have the ability to monitor Java, ActiveX, Visual Basic and other script files to detect and block malicious activity.
- *POP3 Email Scanning:* The programme must have the ability to monitor incoming and outgoing POP3 email traffic and the associated file attachments to detect and alert about virus or other malware threats.
- *Webmail Protection:* The antivirus software should be able to monitor web-based email traffic such as Hotmail, Yahoo! Mail or GMail to detect and block malware in file attachments.
- *Instant Messaging Protection:* The software should monitor instant messaging traffic to detect and block malicious threats. Many worms and other malware can now be spread through instant messaging programs such as AOL Instant Messenger (AIM) or Yahoo! Messenger
- *Automatic Virus Updates:* The antivirus should be configurable to automatically connect with the vendor's site and download new updates on a regular basis.
- *Automatic Program Updates:* The software programs should be configured to automatically check for new updates and download and install them if they are available in order to add functionality to detect new threats.

For added security, the server must also be outfitted with a firewall. At a minimum, an application and circuit gateways (proxies) firewall should be used but a stateful inspection (or smart filter) firewall is preferable.

ICT Service Provider

The EPD will secure the services of an ICT service provider through a competitive bidding process annually. The ICT service provider will design, install

and maintain the a networking and backup solution that meets the Department's needs.

Backup System

The backup system for the electronic data must include both onsite and offsite processes.

Onsite Backup

The onsite backup will involve storing copies of all of the systems and data files on network attached storage (NAS) and external hard drives.

Data stored on the server should be backed up as follows:

- Differential backup daily (Mon.-Fri. beginning at 9 pm) to the NAS which will be located on-site.
- Full backup weekly (Sat. beginning at 1o am) to the NAS which will be located on-site.
- Full backup monthly (last working day of each month) to an external hard drive which will be kept in a cool, dry, fire proof place such as the safe located in the Deputy Director's office.

It is preferable that the Department utilize a NAS system with 4 hard drive bays, which can allow for future expansion. However, a system with 2 hard drives bays would suffice. Regardless of which system is used, a minimum of two 1 TB hard drives must be used with RAID 1 configuration. A RAID 1 configuration would allow for mirroring of the drives. Therefore, if one disk malfunctions, the other can keep working and would contain all of the backed up data. Additionally, the backup files should be compressed in order to effectively utilize the available storage capacity.

The external hard drives may be USB 3.0 or ESATA drive. They will be used alternately to ensure that full back ups for at least two months are available in the event of catastrophic systems failure.

As an additional measure to allow the Department to function in the event of a disastrous system failure, the

seniors of each section should save copies of pertinent files on their computers at the end of each week.

Offsite Backup

A full backup of the server's system files, applications and electronic data shall be made on a weekly basis. The Department will employ one of the following forms of offsite backup:

- remote back up to the servers of the Data Processing Department (DPD); or
- cloud storage (if consistent with Government's policy).

Utilizing the services of the DPD should be free of cost whereas cloud storage will incur a service charge. The EPD will explore these options post-haste.

Back-up Management Procedure & Responsibilities

All of the individuals or entities involved in the backup process should receive adequate training on the data backup process, data restoration process, media rotation, and storage. Moreover, refresher training should be provided every so often.

Backups will be verified periodically:

- On a daily basis, logged information generated from each backup job will be reviewed to identify problems and take corrective action to reduce any risks associated with failed backups.
- Random test restores should be done once a week in order to verify that backups have been successful.

Additionally, the Department will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for management purposes.

The responsibility for ensuring that data is backed up and stored properly will rest with senior management,

the computer operator and the ICT provider. The list below outlines the responsibilities of each group.

Computer Operator Responsible for:

⇒ Maintaining of logs of backup and restore tests

⇒ Performing restore tests

⇒ Notifying senior management of back up errors so that corrective action can be taken or backups re-ran.

⇒ Backing up data to the external hard drives on a monthly basis.

⇒ Reporting significant issues to the senior management.

Senior Management Responsible for:

⇒ Periodically verifying that the backup and restore test logs are accurately maintained and are up to date.

⇒ Ensuring that the external hard drives used to backup are properly labelled and stored.

⇒ Verifying the backup process to the external hard drives.

⇒ Reporting significant issues to the ICT service provider.

ICT Service Provider Responsible for:

⇒ Maintaining the server and NAS in good working order.

⇒ Restoring the system within 3 working days using offsite backed up data in the event of a catastrophic system failure if the destroyed equipment has been replaced by that time.

⇒ Restoring the system within 1 working day using onsite backed up data in the event of non-catastrophic system failure or user error.

⇒ Setting up the server taking into consideration the guidelines outlined herein.

3 BIBLIOGRAPHY

Backup Strategy or Backup Policy. (n.d.). Retrieved 10 30, 2014, from Types of Backup: http://typesofbackup.com/backup-strategy-or-backup-policy/

Data Storage Options. (n.d.). Retrieved 10 30, 2014, from Rebit: https://rebit.com/backup-basics/storage-media-options

I.T, C. (2003). *The Backup Strategy Guide:How to protect your small business from data disaster.*

Incremental vs Differential vs Full Backup. (n.d.). Retrieved 10 31, 2014, from Types of Backup: http://typesofbackup.com/incremental-vs-differential-vs-full-backup/

Individual Data Backup Policy. (n.d.). Retrieved 10 30, 2014, from http://www.aub.edu.lb/it/policies/documents/cns-p-backup-individual-a.pdf

RAID Levels Explained. (n.d.). Retrieved 10 30, 2014, from PC Magazine: http://www.pcmag.com/article2/0,2817,2370235,00.asp

Types of Backup. (n.d.). Retrieved 10 30, 2014, from Types of Backup: http://typesofbackup.com/

What To Look For In Antivirus Software. (n.d.). Retrieved 10 30, 2014, from About Technology: http://netsecurity.about.com/od/antivirusandmalware/a/lookforav.htm

APPENDIX D:

Contract

Contract No.: BARBADOS

PARTIES

THIS AGREEMENT made this **[Insert day (ordinal form)]** day of **[Select month] [Insert year]** BETWEEN the GOVERNMENT OF BARBADOS acting herein through the ENVIRONMENTAL PROTECTION DEPARTMENT (hereinafter referred to as "the EPD") of the ONE PART and **[Name of Company]** a company incorporated and registered under the Companies Act, Cap. 308 of the Laws of Barbados with its registered office at **[Address]** in the parish of **[Parish]** in this Island (hereinafter called "the Consultant") of the OTHER PART.

RECITALS

WHEREAS the Government is desirous of engaging the services of the Consultant to **[Insert Clear & Concise Description of Services to be Provided]** in keeping with the procurement statement of work contained in Appendix I (hereinafter called "the Services");

AND WHEREAS the Consultant submitted a proposal in response to the Invitation for Bid (hereinafter called "the IFB") contained in Appendix I hereto and has agreed to provide the aforementioned Services upon the subject to the terms and conditions hereinafter set forth;

NOW IT IS HEREBY AGREED as follows:-

1. APPOINTMENT OF CONSULTANT

1.1 The Government hereby appoints the Consultant and the Consultant hereby accepts the appointment to provide the Services as set out in the IFB annexed hereto and in keeping with the Proposal submitted by the Consultant also annexed hereto as **Appendix II**.

2. SCOPE OF SERVICES

2.1 The Consultant shall perform the Services as described in the IFB (**Appendix I**).

3. CONTRACT PERIOD

3.1 The Consultant shall perform the Services provided for hereunder during the period **[Full Date]**, **[Insert Year]** to **[Full Date]**, **[Insert Year]**.

4. FEES AND METHOD OF PAYMENT

4.1 The Government will pay to the Consultant a fee of **[Fee in Words] Barbados Currency**, (**BDS$**) for the satisfactory performance of the Services under this Agreement.

4.2 The fee set out above shall be the sole all-inclusive remuneration due to the Consultant for the Services under the Agreement.

4.3 The said fee shall be paid in accordance with the Payment Schedule as set out in the Terms & Conditions (**Appendix IV**).

5. CONDITIONS OF CONSULTANCY

5.1 The Consultant shall carry out the Services required hereunder in accordance with the Terms and Conditions attached hereto as Appendix III.

6. REPORTING

6.1 For the purposes of section 6 of the Conditions the following addresses are specified.000000

If to the Consultant:	If to the Government:
[Name]	[Name]
[Post]	[Post]
[Address]	Environmental Protection Department
	L.V. Harcourt Lewis Building
	Dalkeith
	St. Michael
Telephone:	Telephone: (246) 535-4600
Facsimile:	Facsimile: (246) 228-7103
Email:	Email:

7. APPENDICES

7.1 The following appendices shall form an integral part of this Agreement:

Appendix I	-	Invitation for Bid
Appendix II	-	Proposal
Appendix III	-	Terms and Conditions
Appendix IV	-	Payment Schedule
Appendix V	-	Further Terms and Conditions

IN WITNESS WHEREOF the said parties hereto have executed this Agreement on the date first hereinbefore written.

SIGNED BY)

(print name) *(signature)*

Director)

Authorized Officer,)
Environmental Protection)
Department for and on)
behalf of)
the GOVERNMENT in)
the presence of:)

Signature (*of Witness):*
Name *(print):*
Address:
Calling or Description:

SIGNED BY)

(print name) *(signature)*

[Post])

Authorized Officer of)
[Company Name],)
the Consultant in the)
presence of)

Signature (*of Witness):*

Name *(print):*

Address:

Calling or Description:

Contract No.:

DATED THE DAY OF

20

AGREEMENT

BETWEEN

THE GOVERNMENT OF
BARBADOS

AND

_____

CONSULTANT

APPENDIX III

TERMS AND CONDITIONS

1. DEFINITIONS AND INTERPRETATION

1.1 The following definitions and interpretation shall apply, unless the context otherwise requires, to these Terms & Conditions and the Agreement:-

"Agreement" means the Agreement annexed hereto.

"Consultant" means the individual, firm or company by whatever name referred that is hired by the Government under the Agreement to perform the Services set out in the IFB (Appendix I)

"Deliverable" means anything, as merchandise, that is or can be delivered, especially to fulfill a contract;

"Force Majeure" means Acts of God, strikes, and other labour disputes, lockouts or other industrial disturbances, acts of the public enemy, wars whether declared or not, blockades, insurrections, riots, epidemics, landslides, hurricanes, earthquakes, storms, lightning, floods, washouts, civil disturbances, explosions, any event or situation that cannot be circumvented or avoided by the Consultant through economic means which makes it impossible for the Consultant to carry out its contractual obligations in whole or in part, for a defined or undefined period of time and other similar events not within the control of either party and which by the exercise of due diligence neither party is able to overcome;

"Head of Department" means the person for the time being bearing that respective title in the Department named in the parties clause of the Agreement.

"Services" means the description of the Services required to be performed by the Consultant as provided in the Agreement or in any other document incorporated in the said Agreement.

1.2 Unless the context otherwise requires:

(a) words in the singular shall include the plural and words in the plural shall include singular;

(b) words denoting the masculine gender shall include the feminine and neuter gender also and vice versa;

(c) the headings shall not limit, alter or affect the meaning of any provision.

2. OBLIGATIONS AND DUTIES OF THE CONSULTANT

2.1 The Consultant shall exercise all reasonable skill, care and diligence in the discharge of its duties under the Agreement in accordance with generally accepted standards of professional competence.

2.2 The Consultant shall not engage directly or indirectly in any other business or professional activities in conflict with the performance of its duties under the Agreement or which, in the opinion of the Government, hinder the performance of its duties under the Agreement.

2.3 The Consultant shall submit such plans, reports and other documentation as may be required pursuant to the IFB or other contract document.

2.4 The Consultant shall liaise with the Head of Department or his nominee during the period of the Agreement. All input of the Consultant shall be carried out with and under the overall supervision of the Head of Department.

3. INDEMNITY

3.1 The Consultant shall save and keep the Government harmless and indemnified from and against all claims, losses, damages, costs, expenses, actions and other proceedings made, sustained or brought against the Government which are occasioned by or attributable to an injury, infringement or damage arising from any negligent act or omission of the Consultant in the performance or purported performance of its functions and duties pursuant to the Agreement but not including acts or omissions of servants or agents of the Government.

4. UNDERTAKINGS OF THE GOVERNMENT

4.1 The Government agrees to, where necessary-

(a) Facilitate the acquisition of access to such persons, locations and data as may be required to enable the Consultant to carry out the Services;

(b) Use its best endeavours to facilitate the Consultant's work by coordinating inter-departmental reviews and other inputs into the Services under the Agreement.

(c) Forward to the Consultant its observations and comments on the Consultant's plans, reports and other documentation submitted as may be required by the IFB or other contract document within a reasonable period of receipt of the respective plans, reports and documentation.

5. PROPERTY IN DATA AND MATERIALS

5.1 The copyright and all other proprietary rights whatsoever of all plans, reports, documentation or other material developed by the Consultant for the execution of its obligations under the Agreement vest in and are the absolute property of the Government.

6. REPORTING

6.1 Any notice or request required or permitted to be given or made under the Agreement shall be in writing and signed by the party giving such notice and may be hand delivered or sent by registered mail, postage prepaid or by facsimile with electronic confirmation of uninterrupted transmission by transmission report or the recipient's confirmation by telephone to the sender that the recipient has received the facsimile message to the party to which it is required to be given or made at such party's address specified in the Agreement or at such other address as the party shall have specified in writing to the party giving such notice or making such request.

7. ENTRY INTO FORCE, ASSIGNMENT, MODIFICATION, DEFAULT AND TERMINATION

7.1 The Agreement shall become effective on the date of second signature by the parties unless otherwise specified in the Agreement.

7.2 The Consultant shall not without the prior written consent of the Government assign, sub-contract or transfer any benefits or obligations arising under the Agreement or any part thereof.

7.3 If circumstances arise which call for modification of the Agreement such modification shall be made by mutual consent given in writing.

7.4 Should the Consultant default in fulfilling any of its obligations under the Agreement the Government shall be entitled to determine the Agreement in which case the provisions of section 7.7 below shall apply without prejudice to its rights to claim damages from the Consultant if there are grounds for so doing.

7.5 Neither party shall be liable for any default due to an even of force majeure. Provided that the Government shall be entitled to terminate or suspend the Agreement if the Consultant is unable to perform its duties under the Agreement by reason of any event aforesaid.

7.6 Notwithstanding anything contained in the Agreement, the Government may, at any time by notice in writing, suspend or terminate the Agreement in

whole or in part by requiring the Consultant to stop performing the Services or any part thereof. The period of notice shall be no less than one week.

7.7 The Government shall, in the case of termination or suspension, owe the Consultant or its successors and assigns against surrender of any documents required or necessary for the continuation of the Services, in so far as they are available, such part of the remuneration as corresponds to the state of the Services of the Consultant under the Agreement.

8. TERMINATION FOR CORRUPTION

8.1 The Government may summarily terminate the Agreement in cases where there is evidence that:

(a) the Consultant or its agent has offered or given to any person any gift or consideration of any kind as an inducement or reward for doing, or forbearing to do or having done or forborne to do any action in relation to the obtaining or execution of the Agreement;

(b) the Consultant has shown favour or disfavour to any person in relation to the Agreement;

(c) the Consultant or its agent in relation to any Government contract has committed an offence under the Prevention of Corruption Act, Cap. 144 or any Act replacing the same.

8.2 In the event that the Agreement is terminated in accordance with section 8.1 above the Consultant shall be liable for any loss or damage resulting from such termination, notwithstanding any criminal liability which may thereby be incurred.

9. NON DISCLOSURE

9.1 Any information acquired by the Consultant in the course of its services under the Agreement regarding the policy or processes of the Government shall be treated as secret and confidential and such "Confidential Information" shall not be disclosed to any person, firm orcompany without the prior authority in writing from the Government.

9.2 "Confidential Information" shall not include information which is or becomes public knowledge through no fault, unlawful or wrongful act of the Consultant or is disclosed pursuant to law, court order, or duly authorized subpoena.

9.3 This restriction shall continue to apply after the termination of the Agreement without limit in point of time unless and until such policy or processes shall become public knowledge.

10. GENERAL

10.1 Any and all rights, powers, authorities and discretions expressed in the Agreement to be conferred upon or vested in the Government may be exercised by the Head of Department of the Department named in the parties clause of the Agreement or any other person designated in writing for that purpose by the said Permanent Secretary or Head of Department.

10.2 Any provision hereof which is prohibited, unlawful or unenforceable under the applicable law shall be ineffective without affecting any other provision, or shall be deemed to be severed or modified to conform with such law and the remaining provisions hereof shall remain in full force, provided that the purpose of the Agreement thereby can be effected.

10.3 The Agreement and any annexes or appendices thereto shall supersede all documents and agreements, written and verbal, in respect of the subject matter thereof and represents the entire agreement between the parties thereto.

11. MEETINGS

11.1 Notwithstanding the meetings stipulated in the Agreement, the Consultant shall avail himself to meet with the Head of Department and or his designate if and when the Head of the Department deems such meetings to be necessary.

13. ACCEPTANCE

13.1 Deliverables submitted by the Consultant shall be deemed satisfactory if and only if the deliverable:

(a) Is consistent with the Services contained in Appendix I; (b) Complies with the applicable guidance documentation; (c) Is legible, well formatted and word processed.

APPENDIX IV

PAYMENT SCHEDULE

The payments shall be made in equal installments of dollars Barbados currency at the following times during the contract period provided the reports outlined in the Instructions to Tenderers have been approved by the Environmental Protection Department and an invoice has been submitted.

1st payment – June 30, 2023

2nd payment – September 30, 2023

3rd payment – December 31, 2023

4th payment – March 31, 2024

5th payment – June 30, 2024

6th payment – September 30, 2024

7th payment – December 31, 2024

8th payment – March 31, 2025

APPENDIX V

FURTHER TERMS AND CONDITIONS

1. If at any time Environmental Protection Department wishes to include any additional computer equipment in this Contract it shall so notify the Contractor in writing. The Contractor shall, upon being notified, inspect such additional equipment and submit to Environmental Protection Department a quotation for extending the same services provided thereunder, which quotation shall not be in excess of the Contractor's regular rate then in effect. Upon such quotation being accepted in writing by Environmental Protection Department such additional equipment shall be deemed to be included in Schedule B and the extra service charge agreed shall be deemed to be added to that mentioned in paragraph 3 hereof as from the date the quotation is accepted by Environmental Protection Department.

2. Environmental Protection Department shall notify the Contractor in writing at the commencement of the Contract and when necessary the name(s) of those person(s) authorized to report faults and request services as specified in Schedule A of the Contract on behalf of the Department.

3. Immediately following each visit to Environmental Protection Department the Contractor shall provide Environmental Protection Department with a written report setting out clearly the services performed, the condition of the equipment and details of any repairs considered necessary or advisable and shall obtain the written receipt of Environmental Protection Department for all such reports.

4. The Contractor shall in no way be responsible for any failure to perform any of the services set out herein caused by any act of neglect of Environmental Protection Department or employees of Environmental Protection Department or by any other cause of any kind whatsoever beyond the reasonable control of the Contractor.

5. The Contractor shall employ personnel who shall be fit and competent to perform and carry out the services under this Contract.

6. The Contractor shall provide identification to be worn by its personnel at all times whilst performing the services under this Contract.

7. The Contractor shall not interfere or permit interference by its personnel with any apparatus, object or thing on or in Environmental Protection Department unless such a

cause is necessary for the purpose of this Contract or unless permission has been previously obtained from Environmental Protection Department.

8. The Contractor will not enter or permit entry of its personnel in any building or area at Environmental Protection Department from which its personnel is expressly excluded except permission has been previously obtained from Environmental Protection Department.

9. The Contractor shall be fully responsible for the safe and proper handling of the equipment whilst performing the services under this Contract.

10. The Contractor shall not copy or access any information of the Environmental Protection Department otherwise than as is necessary for the purpose of performing the services under this Contract and shall not deal with or disclose any information so copied or accessed without the written consent of Environmental Protection Department. Any breach by the contractor or its personnel of this clause shall be grounds for termination of this Contract without notice.

11. The Contractor shall not assign or transfer this Contract without the written consent of Environmental Protection Department.

12. This Contract may be terminated at any time without obligation by either party upon thirty days written notice to the other party. In the event this Contract is terminated as aforesaid the Contractor shall refund to Environmental Protection Department a portion of any service charges paid in advance which is reasonable under the circumstances.

13. All notices under this Contract shall be deemed to be duly given upon delivery, if delivered by hand or three days after posting, (Saturdays, Sundays and Public holidays excluded), if sent by registered post to a party at the address set out herein or to such other address as a party may designate by notice pursuant hereto.