P.O. Box 3209,
Houghton, 2041
Block A,
Riviera Office Park,
6-10 Riviera Road,
Riviera

REQUEST FOR PROPOSAL

IT Policy and Procedure Manual

RFP/JHB/2018/015

PROPOSALS TO BE SUBMITTED BY

NOT LATER THAN 12:00 NOON

ON 09 JULY 2018

Terms of Reference

1. Introduction

The Housing Development Agency (HDA) is a national public development agency which promotes sustainable communities by making well located and appropriately planned land available for the development of human settlements. As its primary activity, the HDA assembles state, private and communal land and releases it for development. In addition, HDA provides project delivery support services to organs of state at local, provincial and national level. Informal settlements upgrading, and project management services are a particular focus of the organisation.

2. Scope of Work

The HDA has already developed an IT Strategy and Action Plan for the period 2018-2022. The purpose of the IT Strategy is to align the IT function to the organizational strategy so that information technology is used as a strategic tool to enable the HDA to achieve its objectives.

Part of the IT Strategy is to review, enhance and add additional policy and procedures.

The HDA is seeking a service provider to review, edit and enhance the following;

2.1 IT Policies

Information technology is a critical resource for the HDA. Its utilization must be guided by principles that ensure acceptable use and protection of tangible and non-tangible information assets. Therefore, IT policies are required to address specific areas such as internet usage, email communications, allocation of IT resources, asset acquisition, terms of use, operation, change management, disposal, service level agreements between HDA and internal customers (staff) as well as other stakeholders (vendors, etc).

The following IT Policies needs to be added;

Policy	Description
Acceptable Use Policy	This policy establishes acceptable usage guidelines for all organisation owned technology resources.
Accessibility Policy	The purpose of this policy is to ensure that all employees are presented with an equal opportunity to perform their duties and that all employees can adequately use the required technology equipment for their required occupation.

Policy	Description
IT Auditing Policy	This policy addresses both internal and third-party entities and their ability to conduct an internal technology audit on the organisation.
Data Retention Policy	This policy determines how long data shall be retained under the requirements of the organisation and within the applicable legislated guidelines of South African law.
Encryption Policy	The purpose of this policy is to establish the use of encryption to protect information resources that contain, process, or transmit confidential and organisation-sensitive information.
IT Enforcement Policy	This policy is required to establish enforcement guidelines to ensure that all organisational ICT policies and procedures are adhered to and observed by all departments and individuals including employees, visitors, vendors, etc.
Equipment Configuration Policy	This policy is crafted to create a standard configuration for all organisation technology resources. Organisations generally have variances between the types, makes, models, configurations, builds, versions, and brands of technology resources. It is necessary to standardise the configurations of all technology resources to ensure cohesive operability, and simplify service and maintenance operations and costs.
Guest/Visitor Access & Technology Use Policy	This policy is established and required to set the parameters of guest and visitor access on the organisation's technology resources to ensure that granted access does not compromise the integrity of the system or information contained within the organisation.

Policy	Description
File Sharing Policy	This policy is established to address the requirements for the sharing or transmission of large files with other employees, vendors or 3rd parties. This policy also sets parameters to address illegal file sharing and the penalties for violating intellectual/copyright laws.
Information Sensitivity	This policy is intended to assist employees in determining what information can be disclosed to none-mployees, as well as the relative sensitivity of information that should not be disclosed outside of the organisation without proper authorization.
Physical Security Policy	This policy establishes the physical security guidelines that apply to all computing and networking equipment locations as required for each area of technology within the organisation.
Personally Identifiable Information Policy	This policy establishes and sets the parameters of the definition of Personally Identifiable Information (PII) and indicates what information may be stored of both employees and 3rd parties that interact with the organisation.
Personal Service Technology (BYOD)	This policy sets forth the rules, regulations and requirements which will determine how the organisation will interact and allow access to personally-owned employee or 3rd party technology products.
Remote Access Policy	This policy establishes the official rules to allow users to remotely access and manipulate personally identifiable information, network applications, and other data from off-campus.
Vendor Access Policy	This policy sets forth the parameters for vendors to abide by when accessing the organisation's internal or external network, workstations, or servers.

Policy	Description
Website/Online Presence Policy	This policy establishes the guidelines for the online presence both inside and outside the organisation and is applicable to the defined use of the organisations online platforms i.e. website, news articles, web-publications, social media.
Wireless Communication Policy	This policy establishes all allowances and parameters of wireless data communication devices (e.g., personal computers, cellular/smart phones, PDAs, IoT Devices etc.) connected to any of the organisation's wireless network access points.
Disaster Recovery/ Business Continuity ICT policy	This policy establishes the ICT related requirements to aid the business in the event of a Disaster and ensure business continuity

The following IT Policies need to be reviewed;

No.	Existing Policies	Security factor or requirement currently identified/detailed within policy
1	**ELECTRONIC COMMUNICATION POLICY**	• Transferring Liability to Users (positive) • Tracking Users • Monitoring Users • Censorship • Controlling Usage • Reporting/Whistleblowing
2	**EMAIL POLICY**	• Prohibited Use • Authorised Use • Limiting Liability to the Organisation • Tracking Users • Monitoring Users
3	**EMPLOYEE USE OF COMPANY ASSETS**	• Behavioural Mitigation • Insuring Asset • Asset Register

No.	Existing Policies	Security factor or requirement currently identified/detailed within policy
4	**EMPLOYEE USE OF 3G CARDS**	• Transferring Liability to Users (positive)
5	**WIRELESS POLICY**	• Specified Technology Parameters • Password Protection • Monitoring Devices
6	**VIRTUAL PRIVATE NETWORK (VPN) POLICY**	• Transferring Cost to Users(negative) • Transferring Responsibility to Users (negative) • Transferring Control to Users (negative) **factors are classified as "negative": The implementation and management of a VPN should be managed and configured as part of the role and responsibility of the IT department and not users themselves.*
7	**PASSWORD POLICY**	• Guidelines Specified • Standards Specified
8	**SOFTWARE USAGE POLICY**	• Monitoring Users • Tracking Software • Intercepting Data • Disciplinary Action
9	**WINDOWS SERVER UPDATE SERVICES [WSUS] POLICY & GUIDANCE**	• Guidelines Specified
10	**VIRUS PROTECTION POLICY**	• Guidelines Specified • Transferring Responsibility (positive) • Behavioural Mitigation • Reporting Threats

No.	Existing Policies	Security factor or requirement currently identified/detailed within policy
11	**CHANGE MANAGEMENT POLICY**	N/A
12	**STAFF MOVEMENT (NEW EMPLOYEES, TRANSFERS & RESIGNATIONS)**	• Guidelines Specified
13	**BACKUP POLICY**	• Guidelines Specified • Risk Mitigation
14	**IPAD POLICY**	• Transferring Responsibility (positive)
15	**USAGE OF TELEPHONE AND 3G POLICY**	• Prohibited Use • Authorised Use
16	**LOSS OF IT ASSETS**	• Guidelines Specified • Transfer of Liability (positive)
17	**DATA PROTECTION**	• Guidelines Specified
18	**INFORMATION SECURITY POLICY**	• Responsibilities and roles Identified • Transferring Responsibility • Guidelines Specified • Risks Identified • Confidentiality Clauses Established

No.	Existing Policies	Security factor or requirement currently identified/detailed within policy
19	**IT SERVER ROOM ACCESS POLICY**	• Roles Defined • Responsibilities Defined • User Monitoring

2.2 IT Procedures

IT procedures includes a set of templates for service requests, configuration management, documentation, asset management, operational framework for IT service management, etc.

The following procedures and standards need to be documented;

Procedure	Description
Data Cabling standard	A standards document focused on the data cabling (UTP and fibre optic) infrastructure detailing the product standards and how they must be installed.
Data Networking (wired and wireless) standards	A standards document focused on the data networking wired and wireless infrastructure detailing the product standards and how they must be configured and installed.
Server and storage standard	A standards document focused on the server and storage infrastructure detailing the product standards and how they must be configured and installed.
IP Security end point AV protection standards	A standards document focused on Anti-virus end point protection detailing the product standards and how they must be configured and installed.

3. Evaluation

In order to facilitate a transparent selection process that allows equal opportunity to all production companies, the HDA has a policy for the appointment of consultants that will be adhered to. Proposals will be evaluated in terms of the prevailing supply chain policy applicable to the HDA and it should be noted that proposals will be assessed using the 80: 20 formula for Price and B-BBEE as per the PPPFA.

The following criteria will be used for points allocation for price and B-BBEE compliance on a 80/20 point system:

Table 1 – Price and B-BBEE

CRITERIA	SUB-CRITERIA	WEIGHTING/ POINTS
Price	Detailed budget breakdown	80
B-BBEE (Status Level Verification Certificate)	B-BBEE Level Contributor	20
TOTAL		100

The HDI proposal will be evaluated as per PPPFA regulations.

4. Payment structure

Payment will be made within 30 days of receipt of the materials specified above and as per signed off proofs.

5. General

5.1 Below are compulsory requirements for this service

5.1.1 It is important to note that the successful person will work under the supervision of a HDA representative, abide by HDA's Code of Conduct, and other organizational guidelines.

5.1.2 Kindly complete and submit the following with:

- Registration with the National Treasury Central Supplier Database(CSD Report), if not yet registered use the following link to register : https://secure.csd.gov.za/
- SBD Forms (SBD4, SBD6.1, SBD8 and SBD9) obtainable from HDA Website: www.thehda.co.za/procurement. Under compliance checklist.
- **Valid and Original or Certified B-BBEE Status Level Verification Certificates issued by the following agencies SANAS, IRBA or CCA.**

5.2 Further information regarding technical matters can be sent by an email to: keegan.pillay@thehda.co.za or at Tel: 011 544-1000, and

5.3 Further information regarding supply chain matter and queries can be sent via email to:Sindisiwe.mweli@thehda.co.za or at Tel: 011 544-1000

6 Terms and Conditions.

6.1 HDA undertakes to pay in full within thirty (30) days, all valid claims for work done to its satisfaction upon presentation of a substantiated claim/invoice.

6.2 No payment will be made where there is an outstanding information/work by the service provider/s.

7 Submission of Proposals

7.1 Proposals should be submitted on or before the **09 July 2018** by no later than **12h00** to the following address:

The Procurement Specialist
The Housing Development Agency,
Block A, 6-10 Riviera Road, Killarney, 2193,

7.2 The selection of the qualifying proposal will be at the HDA's sole discretion. The HDA does not bind itself to accept any particular bid/proposal, and the HDA reserves the right not to appoint the service provider.