Terms of Reference for the Hiring of a Consultancy Firm for "Information Security and Vulnerability Assessment"

1. BACKGROUND:

The Government of KP as part of its digital transformation initiative, intends to automate document and file management within the ministries as a first step towards digital governance. The key aims of the transformation exercise are:

- Minimize the use of paper, in a phase-wise manner, eventually transitioning to paperless governance model.
- Improve productivity, efficiency, and transparency of government departments through an automated file management system.
- Improve efficiency of interaction between local, provincial, and federal government entities through the automated file management system and use of secure, innovative
- Information and Communication Technologies (ICT) solutions, including Video Conferencing, email services, shared drive/cloud-based storage facilities
- Improve decision making through data driven governance.
- Create functional and system requirements specifications documents around the recommended changed processes.
- Training Needs Assessment to understand the current state of digital skills and the subsequent training required for adoption of technology initiatives.

Government workflow, approvals and processes through digitization are entering into the realm of cyber space and therefore require mandatory countermeasures to ensure the integrity, confidentiality, and availability. Integrity is a critical property of data that can only be kept intact if data is safeguarded from unauthorized changes or tempering. In addition, data-property of non-repudiation ensures that sender or receiver of data may not deny their actions on data at any moment in time. Critical systems that play a key role in decision making and smooth running of Government operations, such as "Workflow and Document Management System" require that the data at move or at rest should be able to ensure its property of integrity and non-repudiation. To that end, it becomes imperative that appropriate security controls are put in place after a thorough vulnerability assessment, so that the supporting infrastructure, the software itself, and the end points where it is used, are kept safe from the even increasing cyber threats and attacks.

2. OBJECTIVE

Objective of this document is to provide Terms of Reference to the consultancy firm which shall be hired to undergo the vulnerability assessment of the document workflow management system and proposed a robust information security framework as per International best practices.

3. SCOPE:

The consultancy firm is required to conduct a comprehensive review of the network infrastructure, data centers, applications, databases, and end points with internationally approved standard tools and procedures so that vulnerabilities and flaws within the systems are found, documented, tested, and resolved.

4. TERMS OF REFERENCE (TORs):

The review will include (but not limited to)

a. External and Internal network Vulnerability Assessment and Penetration Testing (it will be an end-to-end assessment based on the below list).
b. Application Vulnerability Assessment and Penetration testing around Workflow and Document Management System (DMS).
c. Re-validation upon completion of Vulnerability Assessment & Penetration Testing exercise.
d. Firewall and Routers Configuration Review
e. VPN Configuration Reviews
f. Third Party Interconnection Review
g. Server Security and Configuration Reviews
h. Application Security Configuration Review
i. Remote access and endpoint security assessments
j. Security review of Email Infrastructure.
k. Assessment of the adequacy of controls over the use of various devices
l. Back up, restoration and retention policy and procedures review.
m. Review of Primary and Secondary Data Centre physical and environmental controls.
n. Database Security and Configuration Reviews
    i. Setup and maintenance of system parameters
    ii. Patch Management
    iii. Audit logging
    iv. Logical Access Controls
    v. Performance, Scalability, and Availability

- o. Operating Systems Security (Microsoft and Linux based)
  - i. Setup and maintenance of system parameters
  - ii. Patch Management
  - iii. Audit logging
  - iv. Logical Access Controls
  - v. OS Hardening
  - vi. Performance, Scalability, and Availability
- p. Review of IT processes and IT Management Tools
  - i. IT Asset Management
  - ii. Enterprise Management System
  - iii. Help Desk
  - iv. Change Management
  - v. Incident Management
  - vi. Network Management
  - vii. Enterprise Anti-Virus Management
  - viii. Vendor and SLA management
- q. Security Management
  - i. Security equipment configurations and policies
  - ii. Penetration Testing and Vulnerabilities Assessment of various security zones
- r. Network Assessment of the KP Data Centre.
  - i. Network Architecture review
  - ii. Network Traffic Analysis and base lining
  - iii. Network security review and providing recommendations for better security configuration.
  - iv. DMZ or Network Architecture Designs / Reviews

5. DELIVERABLES:

The deliverables of the assignment comprise of the following within the meaning of the scope of work as defined in these TORs:

- a. Inception Report.
- b. An information security framework based on the leading Standard (e.g ISO 27001, NIST etc.) approved in consultation with all the pertinent stakeholders
- c. Information Security strategy document.
- d. Audit criteria document checklist for ongoing Internal Audit compliance.

e. Test reports of vulnerability assessment of the data center, document workflow management system, and (where the WDMS will be used).
f. Gap Assessment Report covering the complete Information Security Review (as described in SOW/TORs).
g. Operations Guide with Standard Operating Procedures defined for all roles and key events (document).

6. Timelines:

Duration of the assignment will be 18 months.

7. Team Composition:

The following are the required qualification and experience of team memebrs.

Position	Qualification
01 Project Manager / Sr. Manager	- MSc / MA relevant qualification - PMP Certified - 10 Years of Experience
02 Penetration Testers	- BSc Computer Science / Other relevant qualification - Certified Ethical Hacker - 5 years relevant experience
O2 IT Auditor	- BSc Computer Science / Other relevant qualification - CISA and CISM Certified - ISO 27001 Lead Auditor Certified - 7 years relevant experience
Infrastructure Specialist	- BSc Computer Science / Other relevant qualification - CCNA/CCNP Certified - Microsoft Certified Security Engineer/Windows Server Security Administrator - 5 years of relevant experience

8. Selection Method and Qualification

Firm will be selected in accordance with the Consultant Qualification Selection (CQS) method set out in the World Bank’s: Procurement Regulations for Investment Project Financing Goods, Works, Non-Consulting and Consulting Services” (July 2016) revised November 2017, August 2018 & November 2020.

The attention of interested Consultants is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers" July 2016 [revised November 2017, August 2018 and November 2020] ("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest.