TOURISM COUNCIL OF BHUTAN

THIMPHU: BHUTAN

Tender documents for supply and installation

of Unified Threat Management (UTM)

Instruction to Bidders

The Administration & Finance Division, Tourism Council of Bhutan would like to invite quotations from suppliers for supply of **Unified Threat Management (UTM).** You are requested to read the terms and conditions thoroughly and specifications of goods given in the attached list before submitting the tender.

The tender should be submitted addressed to the Director, Tourism Council of Bhutan, Thimphu latest by 12th of February 2018 **before 11:00 a.m. & shall be opened on the same day at 2:00 p.m.**

For further information or clarification, please contact at 02-323251/52.

Terms and conditions

1. **Rate**
   The rate quoted shall be C.I.F Tourism Council of Bhutan, Thimphu inclusive of taxes, transportation, installation/setup and handling charges to be delivered to the Administration & Finance Division, TCB, Thimphu.

2. **Specification**
   You are required to quote as per the requirement/specification mentioned on attached list otherwise your bill shall be rejected.

3. **Period and Rate Validity**
   The selected bidder(s) shall be required to supply UTM with its complete set of accessories and do the proper installation with support service at any time for a period of one year. If the selected bidder fails to supply the goods, the Bid Security shall be forfeited and the work shall be awarded to the second lowest evaluated bidder.

4. **Delivery**
   The selected bidder(s) shall be required to supply complete set of quoted goods and accessories within 15 days from the date of issue of confirmed supply order. In the event of late delivery, penalty shall be charged as per Sl # 5 below.

5. **Penalty**
   If the selected bidder(s) fails to deliver the goods within the scheduled time, penalty shall be charged @ 1% of the total order value per day for another 15 days. In case of further delay, the order shall be cancelled and the Security Deposit shall be forfeited.

6. **Security Deposit**
   The selected bidder(s) shall be required to deposit Security Deposit after receiving the order at the rate of 2% of the total order value in the form of Demand Draft in favor of the Director, Tourism Council of Bhutan within 7 days of the date of order. Failing to deposit the security within time scheduled the order shall be cancelled and the Bid Security lump sum Nu 30,000/- (Thirty thousand) shall be forfeited. On successful

completion of supply of goods, the Security Deposit shall be refunded. On failure to supply the goods within the scheduled time the order shall be cancelled by forfeiting the Security Deposit and awarding the order to the second lowest evaluation bidder.

7. Bid Security

The bid submitted shall be furnished with a Bid Security of Nu 30,000/- (Thirty Thousand) in the form of Demand Draft in favor of the Director, Tourism Council of Bhutan along with the tender. Tender without Bid Security shall be directly rejected. The bid Security of the unsuccessful bidders shall be returned/ refunded after finalization of tender. The bid security of the successful bidder shall be retained with us till the end of the financial year i.e. 30th June 2018. If the successful bidders(s) fail to supply the goods as and when required during the validity period, we shall forfeit the Bid Security of Nu 30,000/- (Thirty thousand) and award the order to the second lowest evaluated bidder.

8. Selection Criteria

The Purchaser reserves the right to select on supplier for all items or to split to more than one.

9. Documents Required

Copy of valid trade license and latest tax clearance certificate should be submitted along with the tender for verification of the eligibility of the supplier. In addition, Integrity Pact Statement should be duly signed with legal stamp along with your official seal. Failing to submit the above documents, the bid shall be rejected.

10. Catalogue

You are required to submit the catalogue for each items bided. If you cannot submit the catalogue, even photographs will suffice.

11. Tax Deduction

2% tax shall be deducted from your bill as per present government rules.

12. Payment

The payment shall be made only after the full delivery of the goods. No part of advance payment shall be made.

13. Note

Please mention confidential and your quotation no. & date clearly on your quotation or your bid shall be rejected.

Annexure:

Unified Threat Management (UTM) or **Unified Security Management (USM),** is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single system, that include network firewalling, network intrusion detection/prevention (IDS/IPS), gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data loss prevention, and on-appliance reporting.

Reasons to install UTM:

1. Proxy server is very old (2005) and gives hardware issues.
2. No firewall with proxy server
3. Data loss (We are not getting full bandwidth due to transmission of unwanted data)
4. No content filtering (We cannot block unwanted sites and downloads)

Note* We have two important systems (Tashel & Regional Permit systems) hosted in our server and have more than sixty network users.

Following are some of the requirements that UTM should provide.

1. **Security (Network Firewall):** A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted
2. **Intrusion detection system:** monitors a network or systems for malicious activity or policy violations.
3. **Gateway Antivirus:** UTM has built in gateway antivirus that prevent/block, detect and remove malicious software and activities in the network.
4. **Content Filtering:** Network administrators can block unwanted sites and downloads.
5. **Data leak prevention:** Data loss prevention software detects potential data breaches and prevents them by monitoring, detecting and blocking sensitive data.

UTM should also offer important security functions as follows:

a) **Anti-Spam:** The Anti-Spam service protects your network from email attacks and infection by detecting known spam IP addresses and matching static spam rules such as URLs filters and spam email addresses.

b) **IPS (Intrusion prevention system):** Protection from a range of known threats is accomplished with single pass inspection using a uniform signature format and a stream-based scanning engine. Intrusion prevention system (IPS) features block network and application layer vulnerability exploits and port scans.

c) **Gateway level Anti-Virus:** The Anti-Virus service helps protect your network from content based threats such as viruses, spyware, and other malware by using signature-based and heuristic-based detection techniques. Features include:

- Anti-Virus and Anti-Spyware service delivered from the network core protects from external and internal attacks
- Multi-layered, real-time protection against known threats and rapid response for evolving virus, spyware, and malware attacks
- Automatic updates of antivirus signatures as and when they become available

d) **Data Leak Protection (DLP):** Data Leak Protection (DLP) identifies sensitive information and blocks transmission to points outside of your network perimeter. A sophisticated pattern-matching engine monitors traffic from multiple applications, such as Web-based email and encrypted instant messaging, and provides audit trails to aid in policy compliance. A wide range of configurable options log, block and archive data, as well as quarantine rogue users.

e) **Content Filtering:** The Content Filtering service helps you limit your user's access to inappropriate sites on the web. The service is constantly updated with URLs and IP addresses of websites that host malware and other harmful content. Additionally, the URLs are classified into web categories such as "Security Risk", "Controversial", etc., thereby helping you control (allow or disallow) internet access, based on web categories.

f) **Device-based policy for application access:** An organization can set specific policies to control which devices can access particular applications and network resources. For example, ensure that laptops are compliant with the corporate image before allowing access to the data centre. Check if the mobile device is up to date, corporate-owned, and fully patched before accessing sensitive data.

g) **Limit unauthorized file and data transfers:** Data filtering features enable your administrators to implement policies that will reduce the risks associated with unauthorized file and data transfers. File transfers can be controlled by looking inside the file (as opposed to looking only at the file extension) to determine if the transfer action should be allowed or not. Executable files, typically found in drive-by downloads, can be blocked, thereby protecting your network from unseen malware propagation. Data filtering features can detect and control the flow of confidential data patterns (credit card or Social Security numbers, as well as custom patterns).

h) **Others:** Any useful features can be added.

Note* Proper user training for operation of UTM to relevant officials should be provided.