# Telkom Tenders

## ERRATUM: RFP00011/2014 TO PROVIDE END POINT SECURITY SOLUTION

**1. TIMELINE OF THE TENDER PROCESS**

1.1 The project timeframes of this RFP are set out below:

| | |
|---|---|
| **Issue Date:** | **2014-03-05** |
| **Closing Date for Questions:** | **2014-03-24** |
| **Bidders Conference:** | **Telkom Towers North, 1st Floor, Erica Conference Room, 2014-03-19, 10h00** |
| **Closing Date:** | **2014-04-17** |
| **Closing Time:** | **11h00** |
| **Validity Period of Submission:** | **120 days** |

**Description:**

The purpose of the RFP will be to select a partner to assist Cybernest with the design, development, implementation and support of a commercially viable End Point Security (EPS) service that is unique and differentiates itself in the South African market.

EPS in respect to the **industry definition** essentially involves the controls deployed to monitor status, activities, authorisation & authentication and threat protection against blended security threats to defined end points that are hosted in the data centre or customer premises. End Points in scope for this RFP/ Service include – physical servers, virtual servers, desktops, virtual desktops, laptops, and mobile devices (essentially any device that can hold data, can access the network or that can be accessed via the network).

The Cybernest EPS Service will be defined by two service model offerings. They include a **Managed Security Service Provider** and **Cloud Managed Security Service Provider** models. The design and development of both service models will include support for End Points located in the datacentre and customer premise. The end points in scope for the datacentre include physical servers, virtual servers and virtual desktops. The end points in scope for customer premises include physical servers, virtual servers, desktops, virtual desktops, laptops, and mobile devices. The service will need to consider integration requirements with billing systems and should conform to the defined security design parameters in place at Telkom and best practice methodologies and techniques.

The Managed and Cloud Service should ensure host based security controls are extended to these defined devices, typical security capabilities that should be supported but not limited to should include host based firewall, intrusion prevention, intrusion detection, anti-virus, anti-spam, content filtering, etc. In addition to the technology security capabilities, respondents should comment on how people and process will be introduced to ensure a comprehensive end point security service is provided to Telkom's external customers.

## 2. Bid Document Collection

The bid document can be collected from the Telkom Tender Office at the following address:

**179 Proes Street, Telkom Tower South,**
**Lower Ground Floor**

Contact Person: Benji Ramatlakana
Contact details: **(012) 311 3364**