APPENDIX 3: IT Infrastructure Guidelines

I. Purpose

This document contains definitions, general information and guidelines for operational functions with regard to the VENDOR IT Infrastructure Guidelines for the IETF community.

II. Definitions

Reference VENDOR Customer Support Guidelines document.

III. Guidelines

A. Collocation

VENDOR has configured the major components of its networks in a manner designed to eliminate any single point of failure. All of the data centers are equipped with uninterruptible power supplies to ensure constant, uninterrupted power availability. Additionally, the data centers are located in different states. Each data center is always "live" with real time mirroring of databases to ensure no interruption of service in the case of an outage at one data center. The VENDOR network has been designed to meet carrier-grade performance standards. Performance results are monitored- on a continuous basis.

1. Data Center Security

The VENDOR Physical Security systems in [Location] protect the VENDOR offices, data center, and Network Operations Center (NOC). The VENDOR Physical Security is comprised of the following systems:

1. Building Door Camera Surveillance System
2. High Security Locks and/or Access Systems
3. Electronic Alarm Systems and Motion Detectors

2. Access (Visitor)

Anyone who does not have authorized access to a restricted area is considered to be a visitor. All visitors must be escorted and signed in. Visitors requiring access to restricted areas must have the following: An VENDOR point of contact (POC), a pre-arranged visit appointment and schedule, a valid photo I.D and when applicable, a written scope of work defining tasks to be performed. Normal working hours in the data center are from 08:00 to 17:00 Monday through Friday. Work performed outside these hours must be

approved by the IT Director. No visitors are ever admitted to VENDOR data centers without advance arrangements and approval.

B. Name Service

1. Standards

VENDOR maintains DNS records for the IETF. DNS change requests will be submitted DNS will be submitted via ietf-action@ietf.org, until further notice by IAD. DNS requests from the IETF and approved by the IAD will be taken 'as-is' and responsibility for the accuracy of the request lies with the requestor.

2. TTL requirements

TTL requirement deviating from the normal DNS template will need to be approved in writing.

3. Other requirements

Additional requirements must be submitted first to VENDOR in the details of the request ticket.

C. Routing

VENDOR data centers are interconnected with dedicated EDIA high-speed optical connections that are provisioned from separate service providers and are physically routed on different paths.

D. Monitoring & Security (Including Spam Filtering)

1. Monitoring

Monitoring of systems is provided by VENDOR staff, which provides tier 1 problem response and troubleshooting.

VENDOR will monitor all pertinent and requested systems, pursuant to requirements outlined in contractual agreements. Additional requests for monitoring will be made via ticket request, and will need to be approved by both VENDOR and the IETF.

a. Alerting

Alerts will be responded to, based on requirements provided.

b. Incident Reporting

All incidents will be provided with a severity number, per the VENDOR Support Standards.

c. Resolution

Appropriate resolution actions and criteria will be followed based on incident severity level.

2. Security

VENDOR will follow the guidelines outlined in this document when administering, supporting and protecting the IETF environment.

a. Data/Server Security

VENDOR will maintain network and server security based on best-practices and data sensitivity level.

b. Spam Filtering

Spam filtering will be administered by VENDOR. Appropriate measures will be taken to provide protection from Spam. VENDOR will take commercially reasonable spam filtering measures, including, at a minimum, those spam filtering measures VENDOR takes to protect other clients and its own internal and external mailing lists.

E. Provisioning core services (FTP & rsync)

1. Time to provision

VENDOR will provision any requested services within the parameters outlined in the SOW and/or any contractual agreement. Any request for provisioning must be provided by the IETF via ticket to VENDOR.

2. Q&A of provisioned services

VENDOR will provide basic testing to ensure that requested services have been provisioned correctly and that services are working within contractual parameters.

3. Emergency Provisioning

Emergency provisioning outside of normal working hours will be done on a case-by-case basis per the contractual requirements.

F. Cooperation & Coordination with Mirror Sites

VENDOR will coordinate any necessary interaction with secondary sites within the IETF network. Guidelines apply to both primary and secondary sites within the IETF network.