Procedure for Testing and Maintenance of Communication Network Security System

1. Introduction:

This document has been prepared in view of the requirements called by MEGC Regulations 2020. As per MEGC guidelines 65.1 (b):

As per the Regulations 59.2, STU shall prepare Procedure on "Testing and Maintenance of communication system".

As per Regulations 62.1, All Users of InSTS shall maintain the communication system availability at 99.9% annually and with a backup communication system, the availability of the communication system shall be 100%.

This document provides procedures for periodic monitoring, testing and maintaining the intra-State communication system developed by STU.

The security testing for the network shall cover the Network forensics (*monitoring and analysis of network traffic for the purposes of information gathering, legal evidence, or intrusion detection*), Network hardening (*disabling non-required services, renaming access accounts and resetting passwords*), Network penetration test (*simulate a cyber-security attack and attempt to uncover security vulnerabilities that might otherwise be discovered by hackers*), Risk assessment, actions to fix problems and to prevent such problems from reoccurring etc. Maintenance plan shall include Preventive maintenance to maintain the regular healthiness of the network.

2. Maintenance:

2.1. Maintenance of fiber network:

All the fibre links including dark fibres shall be periodically tested once in a year and any fibre break / high losses shall be attended in a fixed time frame.

1) Inputs on OPGW and associated Items from transmission line patrolling staff to be given to nodal officer for remedial measures to be taken for immediate rectification.

2) Inputs from Network Management System (NMS) Operators regarding failure of links/high fiber loss etc.

3) Inputs regarding planned expansion (LILO of line), alteration or relocation etc. from concerned line in-charge/substation in-charge/ planning wing of utility

2.2. Maintenance of Communication Equipment (FOTE):

The Preventative/Planned maintenance shall be carried out twice in a year which shall consist of necessary measures to maintain the equipment in proper operating condition. This shall include functional checking, cleaning and necessary repair/replacement/adjustments etc.

The cold trials on protection couplers shall be carried out once in a month for 400 kV lines and once in three months for 220 kV lines.

Continuous monitoring of all the data & speech channels through Network Management System and on observation of any alarms, the checking/testing of the specific circuits shall be taken up.

The NMS operator shall periodically test the alternate / redundant channels and any communication failures shall be intimated to the users for early restoration for ensuring high reliability of the communication network.

The NMS operator shall record any specific and/or all events such as incoming and existing alarms, fault occurrence, action taken for remedies etc. If a module or unit is replaced or repaired, both the new and the replaced or repaired unit is to be recorded in the event report form.

2.3. Maintenance of VSAT equipment :

The procedure mentioned in (2.2) point shall also be adopted for VSAT. The control & protection data should not be connected through the VSAT communication link due to the higher latency in VSAT communication system.

2.4. Maintenance of PLCC :

The Preventative/Planned maintenance shall be carried out twice in a year which shall consist of necessary measures to maintain the equipment in proper operating condition. This shall include functional checking, cleaning and necessary repair/replacement/adjustments etc.

The cold trials on protection couplers shall be carried out once in a month for 400 kV lines and once in three months for 220 kV lines.

The Telecom incharge for particular area shall record any specific and/or all events such as incoming and existing alarms, fault occurrence, action taken for remedies etc. If a module or unit is replaced or repaired, both the new and the replaced or repaired unit is to be recorded in the event report form.

2.5. Maintenance of GPRS :

The nodal officer of AMR project for a particular area shall submit the monthly report of non-availability/ poor reliability of GPRS network to STU. The STU in turn shall take up the matter with concerned for improvement of network or allotment of alternate communication at particular substation.

The purpose of reporting is to summarize the activities performed during the reporting period. The report should provide the information on the performance of the services and describe the current status of the network. The report shall be submitted monthly which must show the trends in the network. By analyzing the report data, management and expert of concerned transmission licensee should be able to focus attention on the areas, where further improvement is needed. A Proper record should be maintained of all the events and activity for reference.

3. Network Security Testing :

The Communication system provider shall ensure that the communication equipment have been got tested as per relevant contemporary Indian or International Security Standards e.g. IT and IT related elements against ISO/IEC 15408 standards, for Information Security Management System against ISO 27000 series Standards etc. The certification shall be got done from authorized and certified agency/lab.

The Communication system provider shall also ensure that the communication equipment has all the contemporary security related features and features related to communication security as prescribed under relevant security standards as mentioned above.

Communication system provider shall also ensure that their Communication system have genuine software, latest updates/patches for Operating system, antivirus and application software. Operating System have inbuilt firewall, regular backup of system files is maintained etc.

Communication system user shall get their network audited from security point of view once a year from a network audit and certification agency as identified by CERT-In. The audit of the network shall be carried once in a financial year."