No.20-271/2010 AS-I (Vol-III)
Government of India
Ministry of Communications
Department of Telecommunications
Sanchar Bhavan, 20 - Ashoka Road New Delhi – 110001

Dated, 26th September 2018

To

All Licensees.

Subject:- ***Minimum Requirements for Security Policy of DoT licensees.***

Following are the instructions on "Minimum Requirement for Security Policy of DoT Licensees" by all the licensees:

1. DoT's licensing conditions issued in May/June 2011 mandates organisational Policy for Security and Security Management of licensees' telecom assets. The Security Policy of DoT licensees' will have minimum provisions as detailed below which shall be applicable for telecom networks, and systems holding customer's data including the endpoints through which such infrastructure and information is accessible. It aims to ensure adequate management directions and support for security arrangements in accordance with service continuity and relevant laws & regulations. Security Policy will provide direction for establishment, implementation, maintenance and continual improvement in Security and Security Management under its scope including security requirements related to vendors'/suppliers' contracts.

2. The Security objectives and the requisite controls to meet defined security objectives including exceptions against individual controls with reasons thereof. It will include, apart from other, the following minimum provision for/to:

a) Organizational set up, roles and responsibilities

- *i) Responsibilities of top management.*
- *ii) Organizational setup, roles & responsibilities for Security Management*
- *iii) Designate a Chief Security Officer(s) for Network Security and Information Security and define his roles and functions*
- *iv) Determine & deploy adequate technical manpower including required resources for the establishment, implementation, maintenance and continual improvement of Security Management.*

b) Guidelines

- *i) Define and implement security risk management system.*
- *ii) Periodic evaluation of the information security performance and effectiveness of the security management viz-a-viz organization's security objectives by monitoring and measurements, feedback mechanism, management reviews, result of risk assessment and status of*

risk treatment plan.

iii) *Auditing their network or get the network audited from security point of view once a year or as and when configuration of network is changed significantly, from a network certification agency which is accredited to carry out the network audit under international standards such as ISO/IEC 27001/ ISO/IEC 27011 including Vulnerability Assessment and Penetration Testing (VAPT). In case, the licensee's network is audited by internal audit team, external audit of the network is mandatory once in a period of three years.*

iv) *Control access to telecom assets, to ensure authorized user access and to prevent unauthorized access to systems and services.*

v) *Ensure that users are accountable for safeguarding their authentication information to prevent unauthorized access to systems and services.*

vi) *Access to telecom assets on need to know basis.*

vii) *Defined change control policy & practices and their implementation.*

viii) *Ensure proper and effective use of encryption techniques/devices to protect confidentiality, authenticity and/ or integrity of information.*

ix) *Ensure adequate protection of telecom assets from power failure and other disruptions caused by failure in supporting facilities for service continuity.*

c) *Control*

i. *Continual improvement of the suitability, adequacy and effectiveness of security management.*

ii. *Identify organizational assets including Critical Information Infrastructure (CII) assets and appropriate protection responsibilities. CII to be protected as per guidelines prescribed by NCIIPC. It shall ensure that telecom assets receive an appropriate level of protection in accordance with its importance to the organization*

iii. *Defined data retention and destruction policies and its implementation.*

iv. *Ensure adequate Heating, Ventilation and Air-Conditioning (HVAC) to maintain equipment room environment within the telecom equipment manufacturer's guidelines.*

v. *Protection of power and telecommunications cables carrying data or supporting information services from un-authorised interception, electromagnetic interference and physical and electrical damage*

vi. *Protection of telecom assets against intrusion of malware.*

vii. *Backup policy to protect against loss of data/information.*

viii. *Ensure that the customer data/information is operated, accessed and remains in the country at all times.*

ix. *Clock synchronization of all elements of network*

x. *Procedure to control the installation, upgradation and maintenance of software on operational systems to ensure integrity of operational systems and to prevent exploitation of technical vulnerabilities.*

xi. *Protection of information in networks, its supporting information*

processing facilities and information transferred within an organization and with any external entity.

xii. *Ensure that security is built in design and is an integral part of information systems and networks across the entire life cycle, including the development lifecycle.*

xiii. *Protection of the organization's telecom assets that is accessible by suppliers/ vendors and maintain agreed level of security and service delivery in line with the supplier/vendor agreement.*

xiv. *Consistent and effective approach to the management of the security incidents, including communication on security events and weaknesses.*

xv. *Security continuity to be embedded in the organisation's service continuity management systems. Ensure availability of telecom facility using sufficient redundancies.*

xvi. *Post attack recovery plan*

xvii. *Development and implementation of crisis management plan*

xviii. *Disaster Recovery plan of operations*

xix. *Compliance with statutory, regulatory, licensing or contractual obligations related to information security and security requirements*

xx. *Induction of only those network elements into telecom network, which have been tested w.r.t network security.*

xxi. *To inspect the hardware, software, design, development, manufacturing facility and supply chain and subject all software to a security/threat check any time during the supplies of equipment as required.*

xxii. *Including all contemporary security related features and features related to communication security as prescribed in relevant security standards while procuring the equipment and implementing all such security features in the network.*

xxiii. *Ensure generation of operation and command logs by telecom network elements and for keeping a record of all operation and maintenance command logs on line for one year and off line for further two years period.*

xxiv. *Protection of operation and maintenance command logs.*

xxv. *Compliance with the terms and conditions prescribed by the Government in respect of Remote Access (RA) operations.*

xxvi. *Compliance to facilities for logging, monitoring and alerting, sufficient to track and prevent all intrusions, attacks and frauds and report the incidents to the Licensor, CERT-Telecom and to CERT-In.*

xxvii. *Root cause analysis of detected incidents*

xxviii. *A suitable agreement with hardware/ software manufacturer/ vendors and supplier of services to ensure that the equipment/ services/ software in the network, have been checked thoroughly for risk and vulnerabilities, backdoors etc. All known and addressable vulnerabilities have been addressed and non-addressable vulnerabilities have been listed with remedial measures and precautions provided. The agreement*

should cover aspects related to security measures like access control, password control and management etc. Clauses addressing the service continuity and service up gradation be included in the agreement, with consequences defined for each party in case of breach, particularly the security breaches.

xxix. *Prepare and document Minimum Baseline Security Standards for Operating Software and applications running on each network element.*

xxx. *Information to licensor regarding major updation and changes within 15 days of completion of such updation and changes.*

xxxi. *Submission of compliance report to DoT on the security related matters indicated in the security audit report by DoT within a period of three months.*

d) *Training*

i) *Periodic trainings, awareness programs, and periodic drills for employees, partners, vendors etc.*

ii) *Conducting periodic reviews & approval for suitability and adequacy of Security Policy.*

e) *Documentation*

Ensure adequate storage, protection and availability of the following documented information:

i. *Security Policy*
ii. *Security Architecture of Telecom network*
iii. *Information security risk assessment & risk treatment processes and their implementation*
iv. *Recruitment processes and employee's record including permanent and local addresses and their pre-employment references. The licensee shall employ only Resident, trained Indian Nationals as Chief Technical Officer, Chief Information Security Officer Nodal Executives for handling interception and monitoring cases and in-charge Soft switch, Central Database and System Administrator/s.*
v. *Controls for effectiveness of the security management*
vi. *Evidence of monitoring, measurement results and management reviews of security management*
vii. *Security Audit programs and audit results*
viii. *Inventory management and classification of information assets and their handling*
ix. *Procedure for responding to information and network security incidents*
x. *Main software updation and changes*
xi. *Supply chain of the products (hardware/software). This should be taken from the manufacturer/ vendor/supplier at the time of procurement of the products*
xii. *Software details and documentation obtained from manufacturer/ vendor/supplier in English language*
xiii. *Operation and maintenance procedure in the form of a manual*
xiv. *Processes for internal and external communication relevant to the Security Management.*

3. The above mentioned provisions will be the minimum requirements for the Security Policy of the Licensees. The licensees are encouraged to have any further

provisions in their security policy to enhance security as deemed fit, because network security is their responsibility

4. The Security Policy of the licensee and MBSS made by the licensee will be the basis of Security Audit of the telecom assets. All the control and checks are to be complied during security assessment. In case of non-compliance, relevant mitigation controls and exceptions shall be considered.

5. Licensee shall be given one-year period to fully implement the above mentioned requirements. Meanwhile, Security Audits could be conducted for gap analysis.

6. These guidelines are subject to review after every two years or on need basis.

Abbreviations

Telecom Assets: *Telecom networks, and systems holding customer's data including the endpoints through which such infrastructure and information is accessible*
NCIIPC: *National Critical Information Infrastructure Protection Centre*
CERT-In: *Computer Emergency Response Team-India.*

25/9/18

(R.K.Soni)
Director (AS)
Phone 23036284

Copy To:

1. Secretary (TRAI).
2. Sr. DDG (TEC)/ Wireless Advisor/ Sr. DDG (DGHQ)/ Sr. DDG (LFP)/ DDG (LFA)/ DDG (Security) and DDG (WPF).
3. Advisor (Economics)/ DDG (CS)/ DDG (DS)/ DDG (A/C) for kind information please.
4. CMD, BSNL/ CMD, MTNL/ CVO.
5. AUSPI/ COAI.
6. Director (IT) may kindly arrange to upload this letter on the website of DoT.
7. All Directors of AS Division.