NETWORK SECURITY POLICY for POLNET

1. NETWORK SECURITY POLICY – ROLE AND STRUCTURE

The POLNET Network security policy is applicable to all Ministries / Departments / Subordinate offices of Government of India and State/UT and Central Police Organisations for handling of unclassified information over POLNET Network. To meet specific needs, ministry / Department / Subordinate office may augment this document by formulation of additional Security Policies. This Network security policy aims at providing secure and acceptable use of the POLNET Network resources. However, this policy does not encompass other security areas such as Physical Security of cyber resources, Data Centers, Mail Servers, Web Servers, etc.

1.1 Network Security Policy : This policy aims to provide controls for secure and acceptable use of client systems Network Administrator is a Department who performs Network Administration functions and provides technical support to the client systems for ensuring their secure and acceptable use.

a) VSAT is connected only in the offices of respective state/UT/central police organization. User shall be responsible for the activities carried out on the client system, using the accounts assigned to them.

b) User shall ensure that the VSAT network is utilized for delivering services and transmission of data voice , fax and video related to Law and Order area.

c) The User shall allow only authorized officials to operate and use VSAT connectivity to ensure security and integrity of data, voice, video and fax transmitted using VSATs. User maintain logs viz., name, date, time, duration etc., of users using Network services through POLNET VSAT.

d) User shall regularly update the patches and updates of OS and antiviruses in VSAT connected computer systems.

e) User shall ensure POLNET VSAT Network is not to be connected to Internet.

f) User nodes shall be subjected to monitoring/filtering for malicious/unauthorized activities.

g) User shall use account with limited privileges on client system and shall not use Administrator Privileges.

h) User shall not leave system unattended. The system should be properly secured with lock and key system whenever it is unattended.

i) User shall not engage in any of the following activities:

   i) Circumventing security measures

   ii) Unauthorised access to system/data /programs.

   iii) Harassing other users by accessing or modifying their data/resources through the network.

   iv) Allowing creation, access, execution, downloading, displaying any form of anti-national, offensive, defamatory, discriminatory, malicious or pornographic material.

v) Making copies of software/data for unauthorized use.

vi) Impersonation, Phishing, Social Engineering, etc.,

vii) Any activity that is unbecoming of a Government Servant.

viii) Network access/connectivity to any other network without prior approval from Network Administrator.

ix) Maintenance or rectification faults in the Network Devices shall be carried out under close supervision of Network Administrator.

x) Network Administrator as a service provider, is responsible for managing the network per location. This policy ensures implementation of controls for secure and acceptable use of client systems by using the administrative privileges.

xi) Network Administrator may temporarily disable the VSAT if the data traffic, virus traffic generated by the VSAT is found to affect the Network performance of other VSATs.

xii) Network Administrator is not responsible for any site related issues at VSAT locations.

xiii) Network Admiistrator shall be responsible for network activities carried out on the client systems, using the administrator account.

xiv) Authentication, Authorisation and Accounting mechanism shall be employed for Network Devices and Network Security Devices.

2. POLNET Network Security Structure : On the basis of ownership of ownership of management of the network, the network security structure is classified in two categories:

2.1: Category I : Security of Network managed by DCPW/Network Administrator like POLNET Hub, VSATs at Hub, VSATs at DCPW locations including Terminals provided at ISPW Stations. It is envisaged that a common Network Security Policy for this category, apart from the security policies envisaged by the individual departments/user organisations.

2.2: Category II : Remote Nodes managed by the respective state/UT /Central Police Organisation. And also at Parliament annexe, NCRB, IB etc.,

3. APPLICATION SECURITY GUIDELINES

Although POLNET Network Administrator is not concerned to the applications envisaged and run over using connectivity of POLNET, yet certain guidelines for safeguarding the applications and information systems are listed below. Insufficient security controls in the application may lead to compromise of an application, system or data processed by the application. Hence the users are required to safeguard the interests of their application with adequate security controls.

3.1 Depending on the sensitivity of the information system and associated data content, application should implement secure authentication mechanism including one or more of, user ID / passwords, hashed passwords, digital certificates, biometrics, etc.

3.2 For providing access to restricted information, application should implement role – based access control, based on the 'least privilege principle'.

3.3 Application should have provision for the user to close the active session.

3.4 Application should enforce suspension / invalidation of a user session after a defined period of inactivity.

3.5 Applications using un-trusted / shared data sources, should implement output validation.

3.6 Error messages provided by the application should be customized to avoid the leakage of internal information.

3.7 POST method should be used for access to sensitive data rather than GET method.

3.8 Audit trails and logging of user activities should be provisioned on the application / database.

3.9 Third party code or downloaded code should be thoroughly checked for security flaws before use.

3.10 Third party security audit and subsequent code hardening of the application should be done before deployment.

3.11 Test accounts, if any, should be removed after use.

4. ASSET MANAGEMENT GUIDELINES

This document provides guidelines for compiling and maintenance of Network resources.

4.1 Asset information updating should be done on yearly basis or if there are any changes, whichever is earlier.

4.2 It is recommended to have an automated tool for compilation and maintenance of Network resources.

5. CLIENT SYSTEM SECURITY GUIDELINES

5.1 Client Network systems are vulnerable to various attacks / intrusions such as malware, unauthorized access, etc. Thus, to protect the client systems, security controls have to be in place. Client System Security (CSS) refers to the software / agents that are installed on the client systems for protection, e.g. Antivirus, systems firewall, etc. Each user should be allocated a separate login account.

5.2 Separate login account should be used for operating at different privilege levels.

5.3 Network device and Network Security Device should have at least two administrators.

5.4 Host name should not reveal make / model of the device.

5.5 Encrypted channel shall be used for Remote administration.

5.6 Unnecessary services should be disabled.

5.7 Unused Network interfaces should be disabled.

5.8 Change management process should be followed for any addition / deletion / modification / on the device.

5.9 Network Time Protocol (NTP) should be configured on the devices.

5.10 Password should be managed as per the Password Management Guidelines of respective user organizations.

5.11 Password should be stored in an encrypted form.

5.12 Configuration of the device should be erased before disposal.

6. **REVIEW:** Network Security Policy may be reviewed by Network Administrator at the time of any change in Network Environment or in intervals of 2 years time span.

****