DRAFT

SWAN Security Policy Guidelines

Feburary 2008

Department of Information Technology
Ministry of Communications and Information Technology
Government of India
New Delhi

SWAN Security Policy Guidelines

Table of Contents

Chapter 1 - Introduction

1.1 About SWANs

State Wide Area Networks (SWANs) in various States and UTs are aimed at providing common communication infrastructure to the State Government bodies, public sector agencies and will have a larger role in processing the G2G, G2B and G2C transactions electronically. SWAN would also provide the Internet connectivity to the proposed Government Network to enable Internet access to its users and to host the Government Applications on the Internet for the public access.

As per SWAN policy, all States/UTs are implementing SWANs under two Options.

Under the first Option, the State/UT will select BOOT operator under Public Private Partnership (PPP) model which will implement and operate the SWAN for a period of 5 years.

In the second Option, the SWAN for the States/UTs would be set up and operated for 5 years by the National Informatics Centre (NIC) of the respective States/UTs.

For the purpose of procurement, implementation, coordination and management of SWANs every state has designated one of its bodies as implementing agency.

Various stake holders in SWAN are:

- DIT, Govt of India
- State Government/UT Administration
- Implementing Agency
- NIC
- NICSI
- Network Operator
- Bandwidth Provider
- OEM/Equipment Supplier
- Third Party Auditor (TPA)
- CERT.In
- STQC

SWANs are typically implemented using a three tier architecture with hierarchical connectivity from State Headquarter to District Head Quarters and to Block Head Quarters. Some of the States have established a four tier nework also by way of incorporating Sub-divisions or Divisions in between. POPs located at these units are connected through dedicated leased lines to form the vertical segment of SWAN. Govt. offices/Public sector agencies at each of these levels are connected to the POPs to form the horizontal segment. A State Data Center (SDC) will be set up at SHQ of every State and connected to SWAN for hosting servers for state wide applications and data. SWAN will be connected to Internet and NICNET from SHQ.

1.2 Purpose of this document

Like any other IT infrastructure SWAN is also surrounded by various information security threats. Many of the surveys conducted in Information Security domain revealed that, there is an equal or greater threat for the Information Assets within the intranet as compared to the threats posed by the Internet. As the designated State agencies design, build and deploy information technology based services, each new project must address the security needed for the effective and secure operation of the information system. Security controls must be an integral part of project planning, development and implementation. Appropriate security controls may consist of both infrastructure and application elements.

SWAN interconnects various Government Agencies across the State and lack of appropriate access controls and monitoring mechanisms may lead to unauthorized access to the information and government transactions. Keeping the above in view, it is vital for the State to establish a Framework and Policy for effectively managing the Information Security for SWAN.

This document aims at providing Guidelines to help the State evolve its SWAN Security Policy and its Implementation Framework. State with the help of its implementing agency may use this document to develope a security document/framework to be followed by the stakeholders. DIT Govt of India, NIC and CERT.in will provide any further assistance that State may need for developing its policy framework for network security using this document.

1.3 Scope of this document

The overall objective of this document is to provide guidance and direction for the protection of SWAN infrastructure against accidental or deliberate damage or destruction. Scope of this document covers:

- Postitioning of SWAN security requirements vis-à-vis Govt. / National Security and Information Security
- Focus on Network Security for SWAN
- Limited Coverage of Application and Data Security

Chapter 2 - Security Policy

2.1 Security Policy Statement

The Government of India recognises its key dependency on the core e-Gov infrastructure created by the State Wide Area Networks (SWANs) and is therefore essential that this infrastructure is secure from destruction, corruption, unauthorised access and breach of confidentiality, whether accidental or deliberate. E-governance plan requires transacting information electronically to provide better services to the citizen. Security requirements are therefore of the utmost importance.

To fulfil the security and risk management needs, Department of Information Technology have developed this Security Policy for State Wide Area network. (A security policy statement is an overall declaration of SWAN security expectations, which will allow effective utilization of SWAN to foster its objectives.) The objective of this Policy Manual is to define standards to ensure that communication infrastructure is secure and is available at all the times.

It is vital that the efforts with security are continued so that the challenges of future e-governance are met successfully to provide efficient and transparent government to the citizen.

2.2 Satandards and Controls

Security standards are derived from the policy statement and provide the overview of necessary control actions needed to achieve the objectives of the policy statement.

2.3 Mandatory Requirements

Mandatory requirements are specific security standards, which are to be implemented at a minimum on SWAN. Implementation of these security standards is a mandatory requirement to safeguard SWAN infrastructure and services.

2.4 SWAN Security Policy Coverage

The security policies, controls and standards contained in this document have been established to cover information and network Security used by State departments. This security policy applies to any stakeholder (State Government, SWAN Operator, SWAN users and TPSLA) who connect using SWAN.

The specific objectives of the "Information Security Policy" are:

- To prevent unauthorized disclosure of information transferred on SWAN (**Confidentiality)**
- To prevent unauthorized accidental or deliberate alteration of information (**Integrity)**
- To prevent unauthorized accidental or deliberate destruction or deletion of information necessary for operations (**Availability)**

The policy will also provide guidance to State to ensure that its State Wide Area network comply with relevant laws and regulations and international standards on information security management.

2.5 Level of Security to be provided

The level of security required is dependent upon the value of the information or the impact of the loss of assets to State/UT, the risks to which they are exposed and the extent to which they are affected by legal and regulatory requirements. The standards provided in this document shall be implemented for SWAN. SWAN Scheme has a provision of Third Party SLA (TPSLA) agency with a role to monitor network performance and security of the SWAN infrastructure. TPSLA Agency will review where existing systems do not comply with the standards; the risks associated with non-compliance and determine what action is appropriate and present a report to the State/UT government on a half-yearly basis.

2.6 Independent Review of SWAN Security

This document defines the policy and responsibilities for information security related to SWAN and its services. Its implementation must be reviewed independently to provide assurance that the practices properly reflect the policy and that it is effective. The State/UT SWAN Security Committee, an independent security officer nominated by State Government or an external agency may carry out such a review on a continuous basis. A full-fledged review must be conducted once in a year by an independent audit function, whether internal or external.

2.7 Responsibility for SWAN Security

The State Government, the SWAN Operator, State and Central Government employees, external contractors, and other third parties, all such stakeholders who require access to SWAN, are responsible for ensuring that SWAN security policies are adhered to and that they operate systems in such a manner so as to ensure its security.

Chapter 3 - Security Organisation

Security Organization structure and the corresponding roles, responsibilities and authorities are defined under this policy. Responsibilities and authorities covered here should be in context to the SWAN Security Management System (SSMS) and other responsibilities of these roles are as per the respective Departmental Roles & Responsibilities.

3.1 Organisational Structure

Typical organizational structure for SSMS could as given below
Chief Information Security Officer
Information Security Manager
Physical Security Manager
System Administrator / NOC Team Head
Location Physical Security Officer

Responsibilities of various titles listed above with respective teams are summarized below:

3.1.1 Chief Information Security Officer

- Overall incharge of SWAN Security.
- Establish, Review & approval of an SWAN Security Policy.
- Ensuring SWAN User security awareness .
- Providing management direction and support for Physical & System Security initiatives.
- Ensuring business continuity as per organization BCP (Business Continuity Plan)
- Organizing Internal & External Audits.

3.1.2 Information Security Manager

- Ensuring adequate Information Security to protect organizational assets across all locations of SWAN.
- Enforcing effective implementation of policies across the organization.
- Reviewing users/departments access rights on a periodic basis. .
- Responding to escalated security incidents and track repeated incidents for taking Preventive actions.
- Ensuring non-disclosure agreements are signed off by users and third parties including contractors and vendors. .
- Organizeing and conducting information securitry training to users across all locations..
- Carrying out risk assessmenton an on-going basis and update management.

3.1.3 Physical Security Manager

- Ensuring adequate Physical security to protect organizational assets across all location.
- Enforcing effective implementation of physical security for SWAN at all locations .
- Budgeting Physical Security Infrastructure as part of Capital budget plan.
- Responding to queries related to Physical Security process and procedures.
- Reviewing physical access rights periodically and taking corrective actions as required.
- Responding to escalated security incidents and tracking repeated incidents for taking Preventive actions.
- Planning and ensuring adequate training to Security staff across all locations.

- Liaisoning with external agencies such as law, cyber crime authorities to meet statutory and legal requirements.
- Recommending changes on Physical and Environmental Security policy.
- Identifying and introduction of new processes to reduce security vulnerabilities.
- Carrying outrisk assessmenton an on-going basis and update management.
- Conducting Fire drills as per the policy. .

3.1.4 System Administrator / NOC Team Head

- Enforcing implementation of policies across the IT Infrastructure.
- Ensuring Disaster Recovery plans are implemented and tested as per the policy .
- Planning and ensuring adequate training on Information Security to IT Managementstaff.
- Providing constructive feedback on improvement of Security Infrastructure.
- Maintenance of records for procedures stated in Security Management System.
- Responding to Security incidents on a timely basis and take corrective actions.
- Maintenance of documents related to Security architecture. .
- Reporting to Management on security violations as defined in procedures.
- Implementation of security products and solutions to minimize security vulnerabilities.

3.1.5 Location Physical Security Officer

- Implementation of Physical Security Policy and procedures as defined in Security Management System.
- Maintenance of records for procedures stated in Security ManagementSystem..
- Reporting to Management on security violations as defined in procedures.

3.2 User Responsiility

- Adherence to Security policies.
- Reporting potential security incidents.
- Helping managers to maintain secured environment.
- To maintance confidentiality and integraty of the data and information.

Chapter 4 - Physical and Environmental Security

SWAN must be secured from unauthorized access, damage or interference. Physical security measures must be in place to ensure the security and integrity of the SWAN infrastructure and services. Environmental exposures are primarily due to naturally occurring events. Common exposures are fire, water damage, earthquake, power failure and air conditioning failure. Environmental security controls must be implemented to reduce exposure to these environmental threats. Security controls in this section would cover:

- POPs (Equipment, Communication Links, Storage Media and Personnel)
- Movement of Equipment
- Inventory Checks, especially for media
- Sensitisation of Horizontal / Department Offices.
- Security Guards and Management of Locks and Keys

4.1 POPs Premises

- Access to Point of Presence (POP) will be controlled and restricted to authorized personnel.
- Signs indicating "Restricted Entry" or a similar message will be prominently posted at all PoP entrances.
- Equipment, Information or Software will not be taken out of premises without prior authorization.
- Administration Team and visitors will be required to wear visible identification (e.g. identification badges, visitor badges) within SWAN PoP premises.
- SWAN Operator will be encouraged to question unescorted strangers not wearing visible identification.
- Personal information processing equipment like laptops etc. will not be allowed inside PoP, unless authorized by the SWAN Information Security Officer. In any case, details of all information processing equipment (like Laptops, PDAs) or Media (like CDs, Tapes, DATs) will be recorded by the security at the time of entry to the premises. These details will be verified at the time of exit.

4.2 Information Storage Media

- All information storage media (e.g. hard disks, floppy disks, DATS, magnetic tapes and CD-ROMs) containing sensitive or confidential data (e.g. configuration files, security logs etc) will be physically secured, when not in use.
- Physical access to magnetic tape, disk and documentation libraries will be restricted to authorized personnel based on job responsibilities.
- Back-up media will be stored in fire resistant safes or cabinets, both onsite and offsite.
- Any personal data processing device or information storage media like cartridge tapes, DAT drives, floppy drives, CD writers will not be allowed to be brought inside the SWAN PoP without formal approval from the Information Security Officer, which need to be logged.

4.3 Video Surveillance and Electronic Access Control System of Sensitive Areas

- State Security Organisation will review security policy for POPs from time to time and decide if there is a need to set up Video Surveillance and/or Electronic Access Control System at sensitive areas. Functional and Operational details of the same will be decided and documented based upon these reviews.

Chapter 5 – Human Resources and Access Control

Employees are one of the most valuable assets of the any organization/department. However, careless, uninformed, or disgruntled employees may cause significant problems of information security. At the same time, employees are ultimately responsible for controlling the dissemination of confidential information. Therefore, policies must be implemented to address the risks of human error, theft, fraud or misuse of facilities and assist all personnel in creating a secure computing environment.

The Human Resource Security Policy consists of the following sections

- Personnel Security
- Security Awareness and training

The Logical Access Controls Policy consists of the following sections:

- User Access Management

Formal processes will be in place to control the allocation of access rights to the Administration & SWAN. User will be granted access based upon the principle of applying the least privilege required for achieving their desired objectives. In this context, the access control Guidelines issued by Intelligence Bureau of the Government of India from time to time for controlling the unauthorized access to secured government premises may also be kept in view.

5.1 Personnel Security

- All SWAN staff will sign confidentiality/ Non Disclosure Agreement (NDA).
- The SWAN Operator will conduct the information security awareness orientation sessions/training for the staff.
- Security roles and responsibilities will be included in job descriptions where appropriate. These will include any general responsibilities for implementing or maintaining security policy, as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.
- SWAN Operator will ensure that files, information/documents, manuals and brochures in possession of the SWAN Staff are recovered in case of the terminations.

5.2 Personnel Security Awareness and Training

- SWAN Stakeholders must be aware of the Information Security Policies and Procedures. To facilitate this awareness there will be an ongoing security awareness program that explains the need for information security and provides the State/central departments with adequate security training. Training program wil cover topics like Introduction to Information Security, SWAN Usage Guidelines, Internet Usage and Virus Controls.

5.3 User Access Control

- User access to SWAN resources at various SWAN PoPs should be granted based on business requirements; on a “need to access” and "need-to-know" basis and the authorization should be obtained as defined in the access control matrix.
- Access to Third party such as Contractors, Customers, Trainees should be permitted after due authorization from Technical Manager/Department Head.
- There should be a formal user registration and de-registration for granting access to Information Systems and Services at all the vertical PoPs.

- User Account creation and deletion process should be followed as per applicable Account Management procedures.
- User should be aware of their access rights and associated responsibilities.
- SWAN User at various PoPs should protect critical information (Documents/Media) under possession, from unauthorized physical and logical access.
- Verification checks of permanent staff should be carried out at the time of job applications.
- Logical access to the SWAN infrastructure should be controlled and monitored.
- Users Access rights to be reviewed on a regular/periodic basis.
- Guest accounts should be removed on installation of systems.

5.4 Password Policy

Password policy is to be enforced for all the critical SWAN resources. Mandatory controls to be followed for the password policy are as follows

- Passwords should be changed every 45 days
- Passwords should be of minimum 8 characters.
- Passwords should be alphanumeric characters with at least 2 numeric characters.
- Blank passwords should not be permitted.
- Default system accounts provided by vendor/ service provider should be renamed upon installation of new systems.
- Password should strictly be kept private and confidential. Passwords should not be shared, coded into programs, stored in an unprotected form in any IT systems (mobile and wireless devices inclusive) or written down.
- Password should not be displayed in plain text while logging in.
- Passwords should be changed immediately during suspected compromise or a wrongful disclosure scenario.
- Initial temporary user passwords should be linked with unique identifiers of a user and should not be guessable.
- Users should refrain from using any option which helps Remember Passwords in any application (at the end user machine or at application level itself) for convenience purposes.
- Any employee/contractor/partner/vendor/service provider or supplier knowing critical system passwords for business purposes at SWAN should be bound by standard non disclosure agreements.
- Password for the Critical System should be changed immediately whenever key personnel administering /having privileged access to the system gets separated from /changes role in the organization.

5.5 Network Access Control

Some of the controls listed here need to be enforced by the application developer and provider. The policy therefore needs to be shared with them too for compliance.

- Basic Hygiene to be checked before provided SWAN access to device/machine. Basic Hygiene check includes installation of all the patches, disables/install services not required, free from virus or malware.
- Network access to be provided to the system/device only after appropriate approvals/authorization.
- Network connectivity to local Servers and to the remote networks/systems should be controlled/ restricted/ monitored by System Administrator/NOC Team.
- Appropriate Network Routing Controls should be defined by System Administrator/NOC Team for protection of SWAN network from external world.
- All networking devices in SWAN should have the capability of implementing Access Control List at Layer 2 to 4 for restricting the access only to the group of eligible people.

- Operating systems and applications should be configured to run only restricted services as required.
- Systems should not permit the information of internal menu /applications, structure system/application identifiers until the log-on process is successful
- Systems should not display help screen (automated), during the logon process.
- Systems should have the log of unsuccessful attempts and designated administrators should review it periodically.
- Systems & Applications should have idle time out parameter set to 30 minutes.
- Systems & Applications should re-authenticate the user after the idle timeout.
- Systems should have system alerts enabled for the console alerts or messages, system log exceptions, and network management alarms as deemed appropriate.
- Customer data and Information should be allowed access through Internet only after approval from Head of SI team.
- Audit trail should consist of unsuccessful log on, Date, Time, IP Address, Login Name. The audit logs should be reviewed as per log file monitoring procedure.
- System utilities should be used only after proper authorization
- Systems should have log-on banner stating that system's use is meant only for authorized users and activities should be monitored.

5.6 Data Encryption Related Policy

- Shared key may be protected against any intrusion by logically and physically securing the device on which the key is stored.
- Shared secret key may be kept offline for retrieval by authorized personnel only, thus maintaining the confidentiality of the same.
- Pre-shared secret key should be of minimum 16 characters and should consist of alpha numeric and special character combination.Complexity of the shared key can vary depending on the intended purpose of usage.
- Relevant audit trails for key management activities should be stored, for verification of the process.
- Passwords to access private keys if any should be adequately protected from unauthorized intrusion.
- Import, export and use of encryption methodologies should be in compliance with applicable laws and regulations.
- Digital certificates based public key infrastructure solutions should be implemented for identified critical applications
- The public and private keys generation and distribution to the User should be unique to the User and constitute a functioning key pair corresponding to the digital certificates.
- Encryption controls should be implemented as required on business critical applications accessible over Internet. Cryptographic keys such as Secret key, Public & Private keys used in the critical IT Systems and Applications should be protected.
- The Pre-shared Key for the Site-Site VPN connection needs to be changed in consultation with the Customer atleast once in Six months.

5.7 Advisories (For Users)

- Its recommended not to use signing and encryption for high volume message attachments especially when working through remote access channels like VPN service or remote access dialup service.
- Users should not store any critical data as attachments in a signed, encrypted email message and hence recommended to store them in separate directories as files in the desktop/laptop.
- Users possessing the private keys (in case of Asymmetric cryptographic methodologies) should be responsible for safety of the keys during usage in the organization.

Chapter 6 - Network Security

Proper network management controls will be established to protect networks from attacks by hackers / unauthorised users from within and outside SWAN network.

6.1 Firewall

Mandatory Controls (Responsibility of NO)

- All internal network connections to external networks, run by other entities, will be protected by firewall
- The firewall design and architecture will be decided based on the security requirements of the internal network
- Deny all traffic by default and only enable those services that are needed.
- If possible, run the firewall service as a unique user ID instead of administrator or root.
- Run the firewall on a hardened and routinely patched operating system.
- Use a secure remote syslog server that makes log modification and manipulation more difficult for a malicious user.
- Ensure to block ports, filter packets & disable un-necessary services from the firewall according to the list released by SANS from time-to-time.
- Firewalls should be configured with the following minimal mandatory rule sets:
  - Block Private IP address segments reaching through Internet
  - Allow restricted services between Internal Network & De-Militarized Zones (DMZs)
  - Deny all services by default and allow required services only.
- Firewalls log files such as; failure/deny should be reviewed on a regular basis.
- Administrative and User access to firewalls should only be provided only on a need basis.
- Configuration changes to the firewall should follow Change Management Request process.
- Adequate care should be taken while applying changes on the firewall to ensure minimal distortion to Production environment
- .No servers will be exposed directly on the Internet

6.2 Intrusion Detection System / Intrusion Prevention System (IPS)

Mandatory Controls (Responsibility of NO)

- Review all policies and signature files on a regular basis.
- It should provide real-time prevention and analysis of attacks.
- Establish a policy for monitoring these systems.
- Harden and secure the IDS component used in SWAN.

Security Considerations for IDS

- Identify all the servers that the organization's security policy deems critical to the enterprise.
- Within each critical server, identify all critical network applications and deploy an application-based intrusion detection system on each one.
- Obtain a current set of attack signatures from IDS vendors and install accordingly. Use a configuration management tool to track the signature file information on all systems.
- Update the policy created above with the list of Access Control Lists that have previously compiled. Ensure that anomaly detection policies reflect the network load histograms collected for each network segment.
- Establish a policy for rotating logs, a copy of which should always be written to remote, removable media.
- Use an SNMP agentand device-generated SNMP traps, when available.
- Provides protection needed during patch latency and ample time to test and deploy patches.

6.3 REMOTE ACCESS

Mandatory Controls (Responsibility of NO)

Remote Access Service (both dial-in & VPN Channelaccess) should be granted to users who meet the criteria given below.

- Users requiring Remote access to be authorized on a need basis.
- Remote access to business information systems across public network (Internet) should be allowed only after successful identification and authentication of users.
- HTTP and Secured HTTP (HTTPS) services should be allowed for those users who are accessing Intranet resources through VPN Channel.
- Exceptions on the above service access restrictions should be duly authorized by Information Security Manager of SI after carrying out a Risk Assessment.
- If remote access account is not used for a predetermined period (say 60 days) the same should be disabled and communicated to the individuals concerned.
- Dial-in and VPN channel services access should have authentication scheme built in with password policy enforced as specified in Access Control policy
- Authentication (User Credentials) used in Dial-in and VPN services should necessarily be encrypted.
- Deny access logs on remote access service should be monitored by Network/Security Operations staff for taking appropriate Preventive actions

Advisories

While using Dial-in connection, following security measures should be taken into account:

- Active Directory account may be created for the vendor with authentication privileges alone, for a definite time period.
- Alternately, Inbound HTTP access alone may be provided to remote desktop support (Cntrl-F1) system.
- Authentication should be provided to login to identified SWAN IT system (IP address) for troubleshooting

6.4 Router, Switch, Hub and Modem Security

Router

- Routers and consoles will be housed in a physically secure location
  - IP spoofing will be prevented for boundary routers as mentioned below.
    - All inbound packets with a source address originating from internal network will be dropped.
    - All outbound IP packets with source addresses other than the internal network will be dropped.
- All unnecessary ICMP traffic will be dropped
- Router passwords will be stored (e.g. in router configuration files) in an encrypted form (such as MD5 Encryption).
- Any user who gains access to the command prompt will not have administrator privileges by default
- Copies of the router configuration files will be restricted to authorised individuals.
- Routers will be set to a VTY and console session time out of 15 minutes.
- No local user accounts should be configured on the router.
- Routers must use TACACS+/ RADIUS for all user authentications.
- The enable password on the router must be kept in a secure encrypted form.
- The router must have the enable password set to the current production router password from the router's support organization.
- Un-necessary services, protocols and ports should be disabled.
- Apply ingress and egress filtering.

- Use SSH for remote administration
- Apply patches and updates regularly and perform test to confirm that the update works properly.
- Define one loopback interface and designate it as the source interface for most traffic generated by the router itself.
- Shut down any interface that is not being used.
- Set access control list entries to prevent inappropriate connections and routing of traffic.
- SNMP should be used only on internal or protected networks.
- Configure the router to build resistance to common attacks (like TCP SYN attack) and intrusions into the network by Route filtering, Packetfiltering and Rate limiting.
- Use identification feature which allows querying a Transmission Control Protocol (TCP) port for identification.
- The preferred and recommended method of securing access to the router is to use an AAA protocol such as TACACS+, RADIUS, or Kerberos. Here the usernames and passwords for all the users who have access to the routers are held at a central location, off the router.
- Logging must be enabled.
- Enable command accounting: all commands (i.e. keystrokes) sent to the router in enable mode are logged in the accounting file on the accounting host.
- Secure IP routing by authenticating the routing protocol used.

Switch

- Control physical access to the switch to only authorized personnel.
- Install the latest stable version of the operating system on each switch.
- Create an ‘enable secret’ password.
- Enable only necessary network services and configure these services securely.
- Utilize SSH/ SSL instead of telnet and set a strong password for SSH/SSL.
- If SNMP is necessary, set a strong community string for SNMP.
- Implement port security to limit access based on MAC address. Disable auto-trunking on ports.
- Disable unused switch ports and assign them a VLAN number not in use.
- Assign trunk ports a native VLAN number that is not use by any other port.
- Configure logging to include accurate time information, using NTP and timestamps.
- Use AAA features for local and remote access to switch.
- Maintain the switch configuration file off-line and limit access to it to only authorized administrators.
- Separate switches should be used for the secure and non-secure sides of the firewall: one switch on the public side of the firewall and one switch on the private side of the firewall. If it is not possible then switch should be partitioned.
- Use dedicated VLAN IDs for all VLAN trunks rather than using VLAN IDs that are also being used for non-trunking ports.
- Use traffic and protocol access control lists (ACLs) or filters preventing untrusted traffic from being filtered, or passed, through the switch.
- Utilize static VLAN configuration.
- Configuring in-band management switch ports only in dedicated and trusted VLANs.
- Use an out-of-band network management platform, separating network managementtraffic from network user,
- Do not use VLAN 1 to carry user or network data traffic.
- Do not use VLAN 1 for in-band or out-of-band management traffic.
- Prune any VLAN, most notably VLAN 1, from all the ports where that VLAN is not needed at all.
- To prevent undesirable protocol interactions within the network-wide VLAN configuration in network, configure VTP domains appropriately or turn off VTP.

- Create a VLAN to collect unused switch ports, and disable unused switch ports and put them in this unused VLAN.

Hubs

- Periodically check hubs to be sure that all cables are connected properly and that no rogue connections exist.
- Configure a managed hub to send an alert when a configuration is modified.

Modems

- Monitor security bulletins from modem vendors for newly discovered security gaps and apply software patches as soon as they are available.
- Ensure that Modems are SNMP enabled for monitoring purpose.

6.5 Wireless LAN

Mandatory Controls (Responsibility of SI)

- The SWAN Wireless system should support Wi-Fi Protected Access (WPA) & Wi-Fi Protected Access 2 (WPA2) providing access control via per-user, per-session mutual authentication and data privacy via strong dynamic encryption.
- Solution support for allowing only legitimate clients to associate with legitimate & authorized network RADIUS servers via authorized access points.
- The wireless system in bridge role should support WPA TKIP algorithm for mutual authentication.
- Should support filtering based on MAC address, IP Address and Ethertype.
- Appropriate risk assessment (business risks and technical risks) should be conducted for the location considered for implementation of Wireless LAN.
- Wireless LAN setup (including the installation and configuration of all wireless LAN components such as Access points) should be duly approved and carried out by System Administrator /NOC Team personnel as applicable in all vertical PoPs.
- Wireless LAN components should be adequately protected by ensuring installation at physically safe places in all locations.
- Appropriate filters for protocols should be implemented between wired network and Wireless network as per the applicability in locations ofimplementation and nature of use of wireless LANs. Services such as Email, HTTP, HTTP (s) and Intranet portals should be allowed for access through these filters.
- Log files of the Access points should be stored and analyzed as per the log file monitoring procedure.
- Wireless LAN users should get duly authenticated to the network using Active directory authentication after proper matching of Service Set Identifiers (SSIDs) between wireless end points and Access points.
- The Access point equipment’s default Service Set Identifiers (SSIDs) should be changed prior to implementation in the Production wireless network.
- Existence of any unknown wireless access point/device or any other packet capturing device should be regularly monitored.
- Access logs should be monitored to see success /failure logon attempts by system Administrator /NOC team.
- Use directional antennas and place access points in the middle of a room rather than near windows.
- Turn off Dynamic Host Configuration Protocol (DHCP) and use static IP addresses instead.This approach is more manually intensive but will prevent an unauthorized user from receiving an IP address and gaining access to the network.
- The transmit power for access points near a building’s peri meter should be turned down.
- Consider using authentication server like RADIUS.

- Use strong encryption by using WPA2
- Ensure management ports are secured.
- Suitable network management tools should be used to monitor the performance, security and availability parameters of Wireless LAN.

Advisories

- Stronger encryption is provided by WPA with TKIP enhancements such as message integrity check (MIC), per-packet keys via initialization vector hashing, and broadcast key rotation and by WPA2 with AES.
- The system should support a variety of IEEE 802.1x extensible authentication protocol (EAP) types including Protected EAP-Generic Token Card (PEAP-GTC), PEAP-Microsoft Challenge Authentication Protocolv2 (PEAP-MSCHAPv2), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), EAP-Subscriber Identity Module (EAP-SIM) & EAP-Flexible Authentication via Secure Tunneling (EAP-FAST).
- User should understand the encryption support capabilities of the wireless cards (in desktops/laptops) before usage in the Wireless LAN network.
- User should not use Wireless LANS for accessing very confidential business applications from public places like Airports, Cybercafes, hotspots (public wireless LANs) etc.

Chapter 7 – Server Security

The physical and logical access should be controlled and monitored for the Server Farm.
Storage security is the group of parameters and settings that make storage resources available to authorized SWAN users and trusted networks - and unavailable to other entities. These parameters can apply to hardware, programming, communications protocols, and organizational policy.

7.1 Server Rooms Physical Security

- All premises should have suitable security perimeters such as an enclosure (wall), gates or suitable access control mechanism.
- Sensitive areas should be located away from public access.
- Access rights to sensitive areas should be periodically reviewed.
- Offices or rooms with suitable locking facility or safes should be considered to secure important information, documents and media.
- Care should be exercised to protect these areas from fire, flood, explosion, civil unrestor any other man-made disaster.
- All premises should follow applicable health and safety regulations and standards.
- Access to sensitive areas should be granted on a "need to know:" basis as defined in Access Control matrix.
- Vacant offices and areas including visiting rooms, board rooms, and conference rooms should be adequately protected.
- Camera, Video equipment should be allowed only after declaration to location security. However, Photography/Videography should be prohibited in the sensitive areas.
- Users/Contractors and Visitors should declare to Security, incoming & outgoing materials on entry and exitto the premises.
- All incoming and outgoing material should be inspected by Security for potential hazards.
- Local Physical Security officer should at his/her discretion enhances the Security measures depending upon the prevailing threats perception governed by Security scenarios.
- Confidential Information (in the form of Magnetic media, Documents) should be appropriately disposed by the owners themselves using Incinerators/Shredder.

7.2 Logical Security

- Implement endpoint protection for SWAN critical servers.This functionality discovers attacks in progress, protects operating systems and applications, and sends alarms to the management console when an exploit is detected.
- A behavior-based endpoint protection solution should be considered as it would block new threats successfully (e.g. the behavioral based endpoint protection software did protect both the Slammer and Blaster worms.
- Internet access should not be allowed from the production servers (e.g. Browsing Internet sites from Servers).
- Implement network IDS for critical network segments, analyzing traffic streams to identify and thwart attacks such as DDoS and hacker activity. The system alerts the management console and/or invokes an automated response within the network infrastructure to shun or block attacks as they are identified.
- Control access between zones with firewalls and routers. Firewalls provide perimeter control for stateful inspection of connections to and from the Server room while blocking access to nonpublic services and hosts through ingress and egress filtering. Routers provide Layer 3 segmentation between zones
- Implement containment with private VLANs on switches. When each host or segment has its own VLAN, security managers can quarantine attacks and prevent their spread to other hosts; hosts on each VLAN can communicate only with the default gateway, not with other hosts.
- Tight access control in the Data Centre through the implementation of AAA on all devices, access controls at Layer 2 to 4 and network admission control.

- In case of virtual firewall solution, every firewall context should have its own CLI and management interfaces.
- The Security devices should be based on realtime, secure, embedded operating system
- Embedded web based management software and command line interface support.
- Operating systems and applications should be configured to run only restricted services as required.
- Systems should have system alerts enabled for the console alerts or messages, system log exceptions, and network management alarms as deemed appropriate.

7.3 Storage Security

- Identify all of the interfaces to storage network.
- Create a separate infrastructure for the out-of-band management and control terminal interfaces to the storage network. If connectivity is required to the corporate LAN, provide it via a firewall or a secure router
- Use secure channels for all remote access (VPN, SSL/TLS, SSH, https)
- Protect both data in flight and data at rest.
- Use FC Zoning, Zoning provides segregation between groups of hosts and disks within a SAN but lacks any form of authentication.
- Restrict access to infrastructure configuration functions.Control access to all of the unused ports in the storage network infrastructure. Only install software and firmware on storage network components from authorized sources,
- Always change default passwords before equipmentis connected to a production storage network.Ensure that strong passwords are required by policy and educate key personnelas to their importance.
- Use FC Security Protocol (FC-SP) as the device authentication which provides stronger means of ensuring device identity.
- Implement logging and intrusion detection.
- Monitor the storage environment.
- Stop external attacks:DOS, viruses, etc.
- Limit installation of storage command line utilities to systems that require them.
- Use access control lists to limit systems that can use storage management capabilities.
- Disable SNMP access if not needed.
- Replace default community names.

Chapter 8 - Malicious code Management

8.1 Centralized Anti-Virus Management

- SWAN should have an antivirus gateway, so that majority of malware can be stopped right from the entry of the network.
- Install and enable antivirus software on all of the potential virus entry points on the network.These include workstations, file servers, email/groupware servers and conduits of Internet traffic like SMTP, HTTP, or FTP servers.
- The latest version of the antivirus with latest definitions/signatures is required to be loaded in all the machines.
- The centralized antivirus server should auto-update virus signatures automatically from the service providers, as and when an update of signature or virus engine is available.
- External media (e.g.Floppy, CDs & USB drives) is one of the most potent medium for transmission of viruses, hence it must not be used in the network.
- Should provide real-time status of the network which informs the administrator immediately if any virus incident occurred.
- View the virus outbreak as a learning experience and fine-tune networkÆs antivirus policy to prevent similar occurrences in the future.
- Anti-virus logs should be maintained for a period of 7-15 days or as determined by the policies .

8.2 Mandatory Controls (Responsibility of SI)

- Antivirus software should be implemented at various levels (e.g.: Desktop, laptops, Email gateways in the Perimeter network) in the network and system infrastructure as part of a layered approach to minimizing malicious code entry in to SWAN Computing environment.
- System Administrator/NOC Team should be responsible for scanning of malicious code for email traffic at the Network Gateway/entry points at all SWAN PoPs.
- Project Manager of SI team should be responsible to ensure malicious code free deliverables to customers
- All the computing resources should be adequately protected with anti-virus software and anti-virus signature updates and periodically scanned for virus existence by System Administrator/NOC Team.
- System Administrator /NOC Team should be responsible to ensure virus free release of new software (including but not limited to customer supplied software) to user.
- System Administrator/NOC Team should certify and ensure provisioning of virus free IT resources, during new implementation of hardware, OS implementation and storage media replacements at various SWAN PoPs.

8.3 Advisories for Users

- User should immediately disconnect his/her desktop/laptop in case of suspicious virus presence and report to local System Administrator/NOC Team helpdesk.
- Users should take adequate precautions against covert channels and Trojan horses, by Using software that are available only from reputable sources
- Inspecting source code before production use if appropriate.
- Controlling access & modification ofsource codes once tested and installed.
- E-mail attachment types such as but not limited to ‘.exe, .bat , cmd, .scr, .pif’ through emails should be blocked for preventing malicious code intrusion in to SWAN Net work.
- Web browsers and email clientsoftware should be configured to avoid unauthorized and automatic execution of Malicious code.

Chapter 9 - Data Backup and Asset Management

All software and data will be backed up regularly in order to ensure that each services and its data can be recovered in the event of SWAN infrastructure / operations failure, loss of service, or loss/corruption of data.

The Data Availability solution that supports intelligent approach to data management by providing comprehensive, cross-platform backup and recovery from the laptop to the mainframe, data replication and policy-driven data management. This solution helps your customers protect those assets that they determine are most important to them and optimizes storage usage.

9.1 Asset Management

Data Owner: The data owner should be Department Head/ Functional head of SI team. Data owner should decide upon the Classification of the data he is responsible for and alters this classification based on the business needs from time to time.

Data Custodian: The Data custodian should hold the responsibility of the maintenance and protection of data. Data custodian's responsibilities should include performing regular backups of data, implementing security mechanisms, restoring data from backup media, and fulfilling the requirements as per Security policies to ensure data protection. Responsibility of data custodian role for SWAN backbone resources should rest with System Administrator/NOC Team and for Project resources should rest with respective Departments.

User: User should be considered as any individual who routinely uses the data for work related tasks. User should be responsible for operational security procedures to ensure the data's Confidentiality, Integrity and Availability to others.
Information assets should be classified in groups with appropriate owners designated for each group of assets.

SWAN Information assets should be as classified as follows:

- System Laptops - System Administrator/NOC User Administrator/NOC Hardware Team
- System Desktops/Laptops System Administrator/NOC User Administrator/NOC Software Team
- System Servers - System Administrator/NOC User Administrator/NOC Hardware Team
- System Administrator/NOC Servers & User Administrator/NOC Software Team
- Switches, System Administrator/NOC Routers, Hubs, Administrator/ Administrator/NOC Team
- Plant & Facilities / Physical Facilities Machinery (AC, security UPS)
- Furniture & Facilities/Physical Fixtures (Tables, Facilities Security Chairs)
- Electrical Facilities Installations

9.2 Backup Management

- Information owner in conjunction with System Administrator/NOC Team should identify the critical Server resources at SHQ that need to be backed up.
- Appropriate backup media should be chosen by Information owner based on the criticality of data and retention period.
- Periodicity of backup (backup schedule) should be determined by Information owner and the backups of Critical server resources should be taken by System Administrator/ NOC Team as per the schedule.
- All backup media should be labeled as per the labeling convention detailed in department backup procedures.
- Backup logs should be regularly maintained and kept up-to-date and it can be in the form of hard or softcopies
- All backed-up resources should be stored in safe (fire-proof cabinet s) and protected place.

- Backed-up data should be checked for its integrity and effectiveness through restoration of selective data.
- Backup/Retrieval logs should be reviewed by the respective system administrator to ensure proper backup.
- Sealed envelopes with signature should be used for transporting media to identified off-site location.

Chapter 10 – Configuration and Change Management

10.1 Mandatory Controls

- Potential impact of any change should be assessed before accepting a change request and Key changes should be authorized and documented by SI team.
- Suitable version control and a change log/directory should be maintained.
- Concerned persons/practitioners should be intimated before implementation of a Change.
- Process should be in place for recovering from 'unsuccessful'changes in SWAN.
- Changes to operational software such as Operating system upgrade, operating system changes, any application module upgrade, Vendor supplied software, Product enhancements, recommended patches should be controlled through change management procedure.
- Changes should be planned and access should be given to only those systems essential to carry out the work.
- Environment for carrying out the tests should be separated from production and changes should be documented.
- Any major changes to operating systems should be a planned activity and appropriate reviews should be done before implementation.

10.2 Advisories

- Authorized users from SI team who can request changes and also the approval mechanism for a change request should be defined.
- Incase of version upgrades of operating systems through patches or software changes, the application should be tested fully for its functionality.
- Modifications to Vendor Supplied products should be discouraged.If changes are warranted, vendors should be intimated to obtain system patches/releases and care should be taken that safety, functionality features are not getting impacted.The original software should be retained and changes should be clearly documented.

Chapter 11- Security Monitoring and Incident Management

Incident management responsibilities and procedures will be established to ensure quick, effective and orderly response to security incidents. Incident management procedures will cover all types of potential security incidents, including the following:

- Information System failure and loss of service due to security breaches or incidents.
- Unauthorized access to the SWAN network
- Deliberate denial of service
- Wide-spread Virus or Worm outbreaks or Server infections.
- Confidentiality breaches

11.1 Security Incident Management

Security incident should be defined as

- Disruption of SWAN services
- Modification of information /data related to SWAN.
- Sensitive information lost
- Violation to SWAN policies
- Unauthorized access to information
- Identity thefts
- Loss of SWAN /client's asset
- Misuse of information & Computing resources
- Incidents related to Physical security such as but not limited to, laptop lost, unauthorized entry into premises, assault

11.2 Security Monitoring & Management – (Guidelines)

- The deployment of the security event monitoring and response system should be hierarchical in nature.The SHQ of SWAN should have a solution to automatically manage the security events and how to respond to them for stopping the impact on the network.
- Should be compatible with all the network security devices of SWAN.
- The system should support central aggregation of logs and events from network devices.
- Should perform event correlation using events and data received.It should be capable of generating a session in real-time by grouping similar event across the network.
- Should be able to determine if threats are valid or have been countered by assessing the entire attack path.
- Should provide feature automate case assignment, investigation, escalation, notification, and annotation for daily operations and specialized audits.
- Should provide standard reports and report generator to modify standard reports or generate new reports to build action and remediation plans, incident and network activity, security posture and audit, as well as departmental reports-in data, trend, and chart formats.
- Should have access to all endpoints across all access methods, including LAN, Wireless, Remote Access and WAN networks.
- Should cover the networks admission, spans across all of the access methods that hosts use to connect to the network and has to expand to cover gateway deployments through WAN links, IP Security (IPSec) remote access, and dialup and local network deployments through the switching and wireless infrastructure.
- Should determine whether the device is running an authorized version of an operating system.
- Should determine if personal firewall, intrusion prevention, or other desktop security soft ware is installed and properly configured as per the corporate policy requirement.
- Should check whether a corporate image of a device has been modified or tampered.

- Should prevent, adapt and provide a distributed response if any new worm and virus outbreaks.
- Should have detailed control of how the mitigation policies are deployed in the network.
- Centralized management console, control over the deployment of the outbreak prevention policies and signatures to the mitigation devices.
- The appliance should be able to support configuration analysis of network devices like firewalls, routers, switches and NAT to deeply understand the network and security policies.
- The security event monitoring and response system should support behavior based and rule based event correlation techniques.
- The security event monitoring and response system should perform matching of the sessions with the rules for identifying incidents from the source to the destination.
- The security event monitoring and response system should have secured web interface for management (HTTPS)

Chapter 12 - Compliance

The operation and management of the SWAN will be subject to statutory, regulatory and contractual requirements. Appropriate policies should be defined and followed to ensure such compliance. The objective for ensuring compliance is to avoid breaches of any criminal and civil law, and statutory, regulatory or contractual requirements. The Compliance Policy consists of the following sections

12.1 Use of Authorized Software

- A list of all software approved for usage in SWAN administration & usage of related services will be maintained by Operator.
- Users are permitted to use only approved software. Use of any other software, without the written permission of Information Security Officer, will be strictly prohibited.
- No unlicensed software, shareware (beyond its period of free use) or pirated software will be used.
- Public Domain Software, in other words, Open Source Software should be used only after proper testing.
- The Operator & State Government will head periodic reviews reports to ensure that no unauthorized software is being used. All software found in violation will be removed immediately.

12.2 Regular Internal Security Audit for Security Policy compliance

SWAN Security audit constitutes both technical and process audits, Technical audits are used to inspect the configuration of systems and examination of network to check whether they are in compliance with the recommended standards.This is made possible by the usage of Tools, Scripts, Checklist and Snapshots. Audits of Process are performed to check whether processes for assurance of information security as mandated by the standards and policies are being adhered to by the respective departments/business units. The audits should be carried out as;

Planned Audit: Based on the risks perceived compliance Team should come up with the audit calendar.This calendar should indicate the organizations/locations that must get covered by the audits.Based on this calendar, Compliance schedules must be created.Draft Monthly Compliance schedules must be sent across to the Auditee and the Auditor and based on their feedback the final Compliance schedule must be published.Auditor should carry out the compliance check based on this schedule.

Unplanned Audit : Unplanned audits basically consist of Implementation checks and Spotchecks.
Auditon implementation checks should be carried out on random basis.A schedule should be drawn and the auditee i nformed aboutthe same.The audit activity must happen immediately based on this schedule.Any new setup or any changes to the existing setup mustbe validated under this category on sample basis.All departments in the organization should be covered.
Audit Tracking and Reporting

- All audits are individually tracked for closures and any significant audit exceptions are reported to the respective department head as well as to the Corporate Internal Audit Committee.
- Audit findings for Planned and Unplanned audits should be based on the type of Risks and auditor will classify the finding as High Risk, Medium Risk or Low Risk.Auditor must classify the findings as Non-compliance to the documented procedure or Inadequacy in the system.
- Final audit report must be published to the Auditee after the completion and sign off of the Draft audit report.

Deliverables Mentioned below are the deliverables from both Planned and Unplanned audits :

- Compliance Report based on ISO 27001 ISMS framework.
- Compliance Report based on Customer request.
- Best practices implementation across organization.
- Root Cause analysis report.

Chapter 13 - Business Continuity Planning

SWAN is a critical infrastructure on which almost all e-Governace applications will run. Therefore, it is very important to ensure that in an unlikely event of a disaster SWAN services must continue. This will not only include telecom links but also data and processes.

13.1 Mandatory Controls (Responsibility of SI)

- Based on assessment of risks, critical business processes involved in SWAN should be identified.
- Events that can cause interruptions to business continuity should be identified.
- Consequence of disasters and loss of service should be analyzed.
- Contingency plans should be developed and business continuity should be ensured within the required time scales.
- Contingency plans should become an integral part of all SWAN related critical business operations and processes.
- Business continuity plan should be documented and should be maintained based on periodic risk analysis.
- Information security requirements should be taken in to consideration, while planning and testing the disaster recovery plans.
- Proper briefing on crisis management should be given to the team members.
- Mock drills should be conducted periodically and ensure update of plans.
- Individuals and Teams who have the decision making authority during crisis should be defined.
- BCP should be kept updated regarding change of roles, names, addresses and contact details.
- Triggers for activating the locations BCPs should be clearly defined.

Chapter 14 – Conclusion

Security requirements of SWAN at various levels are discussed in this document. SWAN being an infrastructure to be used by various NeGP applications within and across States/UTs needs to be accessible to various segments of users and also maintain a high level of security to ensure integrity and confidentiality of information flowing over it. Also it is emphasized that the scope of the SWAN security is limited to the traffic flowing over it and should not be interpreted as State’s Information Security, because that would encompass many more segments and controls.

Secuirty Guidelines presented in this document can be used by the States/UTs to develop their own SWAN Security Policy document which will be used by the Nework Operator and other stake holders to ensure compliance.

There is a necessity of creating an Information Security Organisation at State/UT level to oversee the development, implementation and compliance of SWAN Security Policy. Some of the personnel of this organization may be assigned full time responsibility while the rest may be assigned SWAN security as additional responsibility.

Users need to be sensitized about SWAN security and awareness needs to be created through training and other measures.