4.8 Wide Area Network Security Policy

Policy Statement
The Government of Nova Scotia provides a wide range of services to the citizens of Nova Scotia that require a secure IT infrastructure. Many of the computer systems supporting these services use the Wide Area Network (WAN) to transmit sensitive information such as government financial transactions, personnel and payroll records, and proprietary corporate data. The Government of Nova Scotia is committed to protecting the integrity, confidentiality, and availability of its information systems, the sensitive information these systems handle, and the privacy of citizens’ information, while providing for efficient and effective management of this information.

Definitions

WIDE AREA NETWORK (WAN)
For the purposes of this policy, the WAN is defined to include all lines and devices used to terminate data communication services from a service provider. The WAN may also be referred to as the Provincial Data Network in various service provider agreements and other contracts signed with vendors. WAN devices may include hubs, routers, switches, wireless devices, or other devices. The Security Authority determines whether devices are classified as WAN or not. In this definition, personal computers, file servers, printers, or other Local Area Network (LAN) devices are not generally classified as part of the WAN. (See illustration on following page).

CORPORATE NETWORK
For the purposes of this policy, the Corporate Network includes the WAN, as defined above, as well as LANs including file servers, personal computers, printers, and other computing or data communications devices that are used by any department, office, agency, board, or commission within the Government of Nova Scotia. Any other connected organization is considered an External Entity requiring specific authorization to connect and access the Corporate Network and is required to abide by the WAN Security Policy and Standards, including any revisions, while connected. This definition of the Corporate Network is intentionally broad in scope to provide clear authority boundaries for those charged with its security. (See illustration on following page).

Additional terms used in the body of this policy are defined in the glossary.
Illustration of WAN and Corporate Network

Policy Objectives

The objectives of this policy are to:

- Contribute to a secure WAN environment for all connected departments, offices, agencies, boards, and commissions.
- Provide a uniform security framework to secure the integrity, confidentiality, and availability of information and information systems, at the WAN level.
- Provide, in balance with operational requirements, legislative requirements, and information sharing agreements, the minimum WAN security requirements.
- Raise awareness of information and information technology security needs for all users of the WAN by providing the security principles, requirements, and rules of use.
- Define the clear roles and responsibilities of all users of the WAN, particularly WAN security staff.
• Provide a foundation to develop and implement additional policies and standards as may be required to address specific security issues.

Application
This policy applies to all Corporate Network connected provincial departments, offices, agencies, boards and commissions (Client Organizations), and other authenticated users in an authorized area of the WAN such as municipalities, academic institutions, associations, federal agencies, and commercial organizations (External Entities).

Any content covered by departmental policies also covered by or in conflict with any content in this policy is superceded by this policy. Additionally, this policy supercedes any prior policies related to WAN security such as the Firewall Gateway Policy.

Policy Directives
Policy directives are the minimum mandatory requirements that shall be met by Corporate Network connected Client Organizations and External Entities.

1. IDENTIFICATION/AUTHENTICATION
   a) All accounts, user IDs and devices in the Corporate Network shall be uniquely identifiable.
   b) IT systems within the Corporate Network shall authenticate all users, applications and devices except for those designed specifically for anonymous access. These exceptions require the approval of the Security Authority.

2. ACCESS CONTROLS/AUTHORIZATION
   a) All access points to the WAN shall be approved by the Security Authority.
   b) All physical and logical connections to the WAN intended to provide access by individuals or groups shall be approved by the Security Authority.
   c) All WAN related address changes and configurations shall be approved by the Security Authority.
   d) Any individual, office, or network connected to the Corporate Network shall require all employees to agree, through a signed or electronic agreement, to abide by the requirements outlined in the WAN Security Policy and Standards.
   e) Requests for access to the WAN for an external entity shall be done through the sponsoring government body. The sponsor shall assume all responsibility for the entity being sponsored.
f) Personnel who have access to sensitive information or are responsible for critical IT security functions such as network administrators and technical support staff require security screening.

3. REMOTE ACCESS
   a) Any remote access over untrusted networks shall use technology approved by the Security Authority to secure, monitor, and filter traffic.
   b) All remote access to the WAN shall be authenticated, logged, and restricted to minimize the risk to WAN assets.
   c) Infrastructure Service Management (ISM) of the Chief Information Office must ensure that remote access involving the WAN is monitored to protect the WAN security profile and confidentiality of sensitive information from unauthorized access and disclosure.
   d) Any device which permits user-controlled access to the Corporate Network, such as a wireless modem, is not allowed except where permission is granted by the Security Authority.
   e) All access to the Corporate Network shall occur through approved paths.
   f) All users who use WAN resources remotely shall agree, through signed or electronic agreement, to abide by these requirements.

4. BASTION HOST (FIREWALL)
   a) All communications between the Corporate Network and networks with different security profiles shall be protected by a network firewall approved by the Security Authority.
   b) All bastion hosts and their configurations shall be provided and managed by the Security Authority except where the Security Authority approves Client Organizations to install and manage bastion hosts.

5. TELECOMMUNICATIONS SERVICE PROVIDERS
   a) All service providers contracting with government such as suppliers of data communications or security services shall commit contractually to ensure that the WAN security profile is maintained.
   b) All service providers contracting with government shall have access to the WAN Security Policy and Standards and agree to abide by them and ensure they are enforced within their organization.
   c) Any exception to these directives shall be approved by the Security Authority and included as an addendum to the contract.
6. CONTRACTORS
   a) All contracts or service agreements involving Corporate Network facilities, configuration, management or any other application or server residing on the network shall include appropriate security clauses ensuring compliance with the WAN Security Policy and Standards.
   b) All persons and organizations contracting with government (i.e., consultants, third party sub-contractors, and casual and student employees) shall have access to the WAN Security Policy and Standards and agree to abide by them.

7. PHYSICAL AND ENVIRONMENTAL SECURITY
   a) An adequate environment (e.g., temperature, humidity, backup power supply) shall be provided to ensure optimum operation of the WAN and common infrastructure equipment as specified in the WAN documentation.
   b) Physical controls shall be implemented to prevent unauthorized access to Corporate Network equipment including routers, switches, wiring racks, and network access servers.
   c) The Security Authority shall have input into and final approval of all site design where WAN connectivity is being provided.

8. TIME SYNCHRONIZATION
   a) All devices on the Corporate Network shall synchronize with a common central time source.

9. REVOCATION/TERMINATION OF WAN PRIVILEGES
   a) The Security Authority shall take appropriate action, including termination of any connection or activity, at any time where the Security Authority feels the security of the WAN is or could be severely comprised. When circumstances permit, the Security Authority shall consult with the application owner prior to taking action. The Security Authority shall make a full report of the actions taken and the reasons for such actions.

10. CHANGE CONTROL
    a) All planned, scheduled changes to the WAN (power up, power down, configuration changes, and reset) shall be performed or authorized by the Security Authority.
    b) A change control process shall be used to assess the security impact of major system upgrades and to support re-certification and accreditation. The change control process shall ensure that all system configurations and modifications are documented and retained in a secure environment for audit or future risk management considerations.
11. SECURITY RISK MANAGEMENT MECHANISMS AND PLANNING
   a) Security risk management based upon due diligence and due care shall be the
   primary basis to determine WAN security safeguards and residual risk, and to
   maintain the accredited WAN security profile.
   b) Re-assessments of the security profile shall take place if risk, system, or other
   relevant technological or organizational changes occur.
   c) Before implementation, all new systems as well as additions, deletions, or
   alterations to existing systems shall be reviewed to ensure that the security
   profile of the Corporate Network is not compromised by the change.

12. CERTIFICATION AND ACCREDITATION
   a) IT system security certification and accreditation shall be performed on the
   Corporate Network (including all hardware and software that comprises the
   Corporate Network) throughout the planning, implementation, and operations
   life cycle.

13. SECURITY LOGS AND RECORDS
   a) Appropriate logs shall be kept and reviewed as prescribed by the Security
   Authority. All actual or suspected security incidents shall be recorded and
   reported to the Security Authority.

14. INCIDENT REPORTING AND INVESTIGATION
   a) All Corporate Network security incidents shall be reported and investigated
   immediately by the infrastructure or application owner, Client Security Officer or
   designate, the Security Authority, or others as appropriate. The Security Authority
   shall notify other Client Security Officers who may be affected.
   b) The Security Authority may also conduct a self instituted secondary investigation
   as requested by the infrastructure or application owner, Client Security Officer or
   designate to determine if there are additional security issues and the appropriate
   solutions.

15. SECURITY INFORMATION/DOCUMENTATION
   a) WAN infrastructure shall be documented as required by the Security Authority
   from time to time. The Security Authority shall be given access to this
   documentation on request to support WAN design security issues, disaster
   recovery operations, change control processes, diagnostic or hacker investigations,
   visual inspections, and security audits of the WAN infrastructure.
b) WAN security information and documentation including configuration, backups, and diagnostic information shall be password protected, physically stored under lock and key, and only released on the approval of the Security Authority. If located at a contractor site the protective details and obligations shall be addressed in the contract.

c) Security information and documentation to be discarded, and which contains sensitive information such as passwords and IP addresses, shall be irretrievably destroyed in a secure manner by shredding, permanent electronic deletion, or by other means approved by the Security Authority.

16. MONITORING/SURVEILLANCE AND PRIVACY
   a) The Security Authority shall monitor the WAN for performance and security purposes.
   b) Monitoring initiatives designed for the WAN shall operate within the legislated requirements for protection of personal privacy.
   c) Access or monitoring of LAN segments shall be in co-operation with network administrators.
   d) No person shall operate sniffers or other monitoring devices on the Corporate Network without the prior knowledge of the Security Authority.
   e) Corporate Network monitoring shall not involve reading data content unless it is required in the performance of duties.
   f) Where there is reason to believe that an individual is engaging in inappropriate activity on the Corporate Network the content of individual files may be read. This would only happen in an approved investigation by appropriate authorities.
   g) Any investigation of data content shall be conducted in accordance with applicable human rights, and any applicable provincial and federal legislation.

17. SECURITY TRAINING
   a) The Security Authority shall provide training to all ISM staff, Client Security Officers or designates, and others as necessary on WAN Security Policy and Standards including interpretation and application.
   b) Client Organizations are responsible for the WAN Security training within their organization, and for any External Entities sponsored by them, required to ensure performance of the security responsibilities outlined in the WAN Security Policy and Standards.
Policy Guidelines
The Wide Area Network Security Standards, WAN Security Processes, and WAN Security Intranet web site <http://wansp.gov.ns.ca> are supplements to this policy providing interpretation, technical standards and best practices, and guidance on implementation, risk, and compliance. These shall be amended from time to time as necessary to keep current with changing technology and respond to new threats to the WAN.

Accountabilities

DEPUTY MINISTER/DEPUTY HEAD
The Deputy Minister/Head of each Client Organization is accountable for the overall security of all information within their jurisdiction.

DEPUTY MINISTER OF THE CHIEF INFORMATION OFFICE
The Deputy Minister of the Chief Information Office is additionally accountable for the strategic development and analysis of policy, standards, and processes for information security.

SECURITY POLICY CO-ORDINATOR
The Security Policy Co-ordinator is responsible for developing, monitoring, and proposing revisions to the WAN Security Policy and Standards in co-operation with WAN stakeholders.

SECURITY AUTHORITY
The Security Authority is responsible for operational WAN security management and directs the implementation of the WAN Security Policy and Standards in co-operation with ISM, Client Security Officers or designates. The Security Authority evaluates and responds to all requests related to WAN access, services and security.

CLIENT SECURITY OFFICER OR DESIGNATE
A Client Security Officer or designate is the individual(s) assigned within each Client Organization to carry out security requirements and communications for their Client Organization and to work in co-operation with the Security Authority to ensure compliance with the WAN Security Policy and Standards.

CLIENT ORGANIZATION
A Client Organization is any department, office, agency, board, or commission in the Government of Nova Scotia connected to the Corporate Network and is required to abide by the WAN Security Policy and Standards.
**EXTERNAL ENTITY**
An External Entity is an organization having business with government, sponsored by a Client Organization and authorized by the Security Authority, connected to the WAN. The External Entity shall agree to abide by the WAN Security Policy and Standards.

**MANAGERS AND DELEGATED STAFF**
Managers and delegated staff, in addition to specific responsibilities cited above, shall have other specific responsibilities for such WAN aspects as availability, network upgrade and maintenance, security monitoring and incident reporting.

**ORGANIZATIONS HOSTING WAN FACILITIES**
Organizations hosting WAN facilities such as routers, firewalls, wiring closets and other related components shall ensure that physical protection of WAN assets meets the WAN Security Policy and Standards.

**Monitoring** (of the WAN Security Policy)

**DEPUTY MINISTER/DEPUTY HEAD**
The Deputy Minister/Head of each Client Organization is responsible for overall compliance with the WAN Security Policy and Standards.

**SECURITY POLICY CO-ORDINATOR**
The Security Policy Co-ordinator shall monitor WAN Security Policy implementation. This responsibility includes evaluating the suitability and effectiveness of the policy and standards. The Security Policy Co-ordinator shall co-ordinate any necessary remedial action to address issues reported by the Security Authority in the annual WAN security report. The Security Policy Co-ordinator shall also ensure that the policy and standards are formally reviewed at least every two years.

**SECURITY AUTHORITY**
The Security Authority is responsible for monitoring the operational security of the WAN ensuring that the established security profile is maintained and that changing environments, potential threats, and evolving technology are addressed. The Security Authority shall report annually to the Security Policy Co-ordinator on the WAN security environment, identified issues and security incidents, and the effectiveness of the WAN Security Policy.

**INFRASTRUCTURE SERVICE MANAGEMENT (ISM)**
ISM shall monitor compliance with the WAN Security Policy and Standards for all IT systems within their jurisdiction. ISM shall notify the Security Authority and the Security Policy Coordinator to request a policy review.
CLIENT SECURITY OFFICER OR DESIGNATE
The Client Security Officer or designate shall monitor compliance with the WAN Security Policy and standards for all IT systems within their jurisdiction. The Client Security Officer or designate shall notify the Security Authority and the Security Policy Coordinator to request a policy review.

References
Freedom of Information And Protection of Privacy Act
Government Records Act
Human Rights Act
Public Archives Act
Members and Public Employees Disclosure Act
Conflict of Interest Policy (Management Manual 500, Chapter 9, Policy 9.3) and any other applicable legislation, provincial or federal

Standard for Administrative Records/Standard for Operational Records (STAR/STOR) and any other applicable policies or procedures which contain specific requirements for the production of, access to, and retention and disposition of records.

Appendix
4-D  Glossary

Enquiries
All enquiries, requests, or comments should be forwarded to

Director, Corporate Information Management Program
Corporate Information Strategies
Chief Information Office  (902) 424-2915

Approval date:  April 1, 2002
Approved by:  Treasury and Policy Board, Business and Technology Advisory Committee
Effective date:  October 1, 2004
Administrative update:  February 7, 2013
Appendix 4-D

Glossary

ACCESS CONTROL
A set of procedures performed by hardware, software and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.

ACCREDITATION
Approval by the responsible manager for the operation of an information technology system using a particular set of safeguards.

AUTHENTICATION
The process of determining whether a person, workstation, system or procedure is eligible to access specific information, or to perform certain operations. Password validation, for example, is a form of authentication. Authentication may also be a measure meant to validate a transmission or message and the authority of the originator.

BASTION HOST
A server that is hardened against attack and can therefore be used as a critical component of network security. Firewalls and screening routers are examples of bastion hosts.

CERTIFICATION
An examination by qualified personnel of an information technology system’s implemented security safeguards against the system’s security requirements.

CLIENT ORGANIZATION
See Accountabilities.

CONFIDENTIALITY
The sensitivity of information or assets to unauthorized disclosure, recorded as highly confidential, confidential or protected, each of which implies a degree of injury should unauthorized disclosure occur.
CONTRACTOR
A third party involved in the direct management of the WAN or any part of it, quite often under a WAN management or data communications, service agreement. Contractors are required to abide by the WAN Security Policy and Standards.

CORPORATE NETWORK
See Definitions.

DUE CARE
Reasonable attention or caution which could be expected from an average person under the circumstances.

DUE DILIGENCE
A measure of prudence which could be expected from a reasonable and prudent individual having responsibility for some aspect of security risk management. It carries with it a higher level of responsibility than “due care”.

EXTERNAL ENTITY
See Accountabilities.

FIREWALL
A network security device positioned between networks with different security profiles that ensures all communications attempting to travel between the networks conform to the configured security profile.

INTEGRITY
The quality or condition of being accurate or complete.

MODEM (MODULAR-DEMODULATOR)
A device that converts digital signals used by computers and analogue signals used by the telephone or related telecommunication system which enables computers to communicate remotely. In the WAN Security Policy and Standards, a modem includes any telecommunications device such as a dial-up modem, cable modem, dedicated line modem, wireless device or digital subscriber line (DSL) device.

MONITOR
The activity to ensure that information and assets, or the safeguards protecting them, are checked by security staff or electronic means with sufficient regularity to satisfy the WAN Policy and Standards.
SECURITY PROFILE
A minimum acceptable level of security for the WAN established by the implementation of the WAN Security Policy and Standards.

SECURITY AUTHORITY
See Accountabilities. All references to the Security Authority in this document means the Security Authority or a delegate appointed by the Security Authority from time to time.

SECURITY INCIDENT
An occurrence or situation that results in a compromise of sensitive information, assets, functionality, or a loss of availability or integrity.

SECURITY RISK MANAGEMENT
The process by which resources are planned, organized, directed and controlled to ensure the risk of operating an IT system remains within acceptable bounds at optimal cost.

SERVICE PROVIDER
A third party involved in the direct management of the WAN or any part of it, quite often under a WAN management or data communications contract. Exceptions to the WAN Security Policy and Standards, if applicable, shall be documented in the service agreement.

TIME SYNCHRONIZATION
Process of insuring that all devices on the WAN have the same time to insure the accuracy of records and logs.

THREAT
Any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets, services, or injury to people. A threat may be deliberate or accidental.

THREAT AND RISK ASSESSMENT
An evaluation, based on the effectiveness of existing or proposed security safeguards, of the chance of vulnerabilities being exploited.

UNTRUSTED NETWORK
A network, such as the Internet, that has no basis for a user to have any confidence and assurance in its inherent security.
WIDE AREA NETWORK (WAN)
See Definitions.