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)

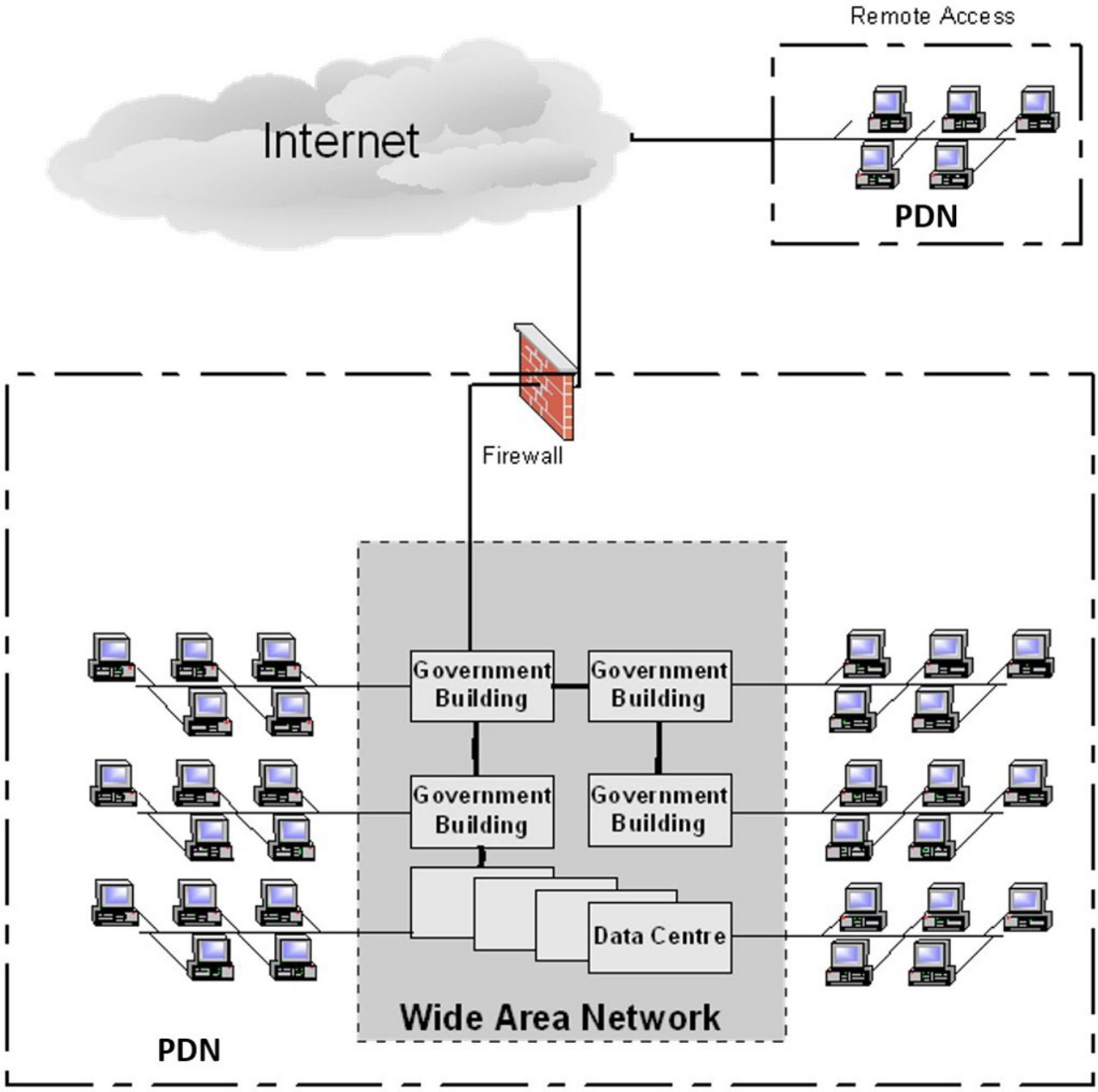
For the purposes of this policy, the WAN is defined to include all lines and devices used to terminate data communication services from a service provider. The WAN may also be referred to as the Provincial Data Network in various service provider agreements and other contracts signed with vendors. WAN devices may include hubs, routers, switches, wireless devices, or other devices. The Chief Technology Officer 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).

PROVINCIAL DATA NETWORK (PDN)

For the purposes of this policy, the PDN 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 PDN and is required to abide by the WAN Security Policy and Standards, including any revisions, while connected. This definition of the PDN 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 PDN



This is a conceptual illustration to differentiate the WAN from the PDN. It is not intended as an accurate depiction of the complexity of the PDN.

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.
- 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 PDN connected provincial departments, offices, agencies, boards and commissions (Client Organizations), and other authenticated users (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.

Policy Directives

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

1. IDENTIFICATION/AUTHENTICATION

a) All accounts, user IDs and devices in the PDN shall be uniquely identifiable.

b) IT systems within the PDN shall authenticate all users, applications and devices, Exceptions require the approval of the Architectural Review Board (ARB)

2. ACCESS CONTROLS/AUTHORIZATION

a) All points of entry to the WAN shall be approved by the Chief Technology Officer.

b) All physical and logical connections to the WAN intended to provide access by individuals or groups shall be approved by the ARB.

c) Any individual, office, or network connected to the PDN 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.
d) 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.
e) 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 Chief Cybersecurity Officer 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) The Chief Cybersecurity Officer must ensure that remote access involving the WAN is monitored to protect the WAN security profile.
d) Any device which permits user-controlled access to the PDN, such as a router, is not allowed except where permission is granted by the Chief Technology Officer.
e) All access to the PDN 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. FIREWALL

a) All communications between the PDN and networks with different security profiles shall be protected by a network firewall approved by the Chief Cybersecurity Officer.
b) All firewalls and their configurations shall be provided and managed by the Chief Cybersecurity Officer.

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 Chief Technology Officer and included as an addendum to the contract.

6. CONTRACTORS

a) All contracts or service agreements involving PDN 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) Physical controls shall be implemented to prevent unauthorized access to PDN equipment including routers, switches, wiring racks, and network access servers.

b) The Chief Technology Officer and the Chief Cybersecurity Officer 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 PDN shall synchronize with a common central time source.

9. REVOCATION/TERMINATION OF WAN PRIVILEGES

a) The Chief Cybersecurity Officer shall take appropriate action, including termination of any connection or activity, at any time where the Chief Cybersecurity Officer feels the security of the WAN is or could be severely comprised. When circumstances permit, the Chief Cybersecurity Officer shall consult with the application owner prior to taking action. The Chief Cybersecurity Officer 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 (system upgrades, configuration changes, and reset) shall be authorized by the ARB.

b) 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) Before implementation, all new systems as well as additions, deletions, or alterations to existing systems shall be reviewed by the ARB to ensure that the security profile of the PDN is not compromised by the change.

12. SECURITY LOGS AND RECORDS

a) Appropriate logs shall be kept and reviewed as prescribed by the Chief Cybersecurity Officer. All actual or suspected security incidents shall be recorded and reported to the Chief Cybersecurity Officer.

13. INCIDENT REPORTING AND INVESTIGATION

a) All PDN security incidents shall be reported and investigated immediately by the Chief Cybersecurity Officer. The Chief Cybersecurity Officer shall notify others who may be affected.

b) The Chief Cybersecurity Officer may also conduct a self instituted secondary investigation as requested to determine if there are additional security issues and the appropriate solutions.

14. SECURITY INFORMATION/DOCUMENTATION

a) WAN infrastructure shall be documented as required by the Chief Technology Officer from time to time. Access to this documentation will be provided 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 and only released on the approval of the Chief Technology Officer. 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 Chief Data Officer.

15. MONITORING/SURVEILLANCE AND PRIVACY

a) The Chief Technology Officer shall monitor the WAN and the PDN for performance purposes.

b) The Chief Cybersecurity Officer shall monitor the WAN and the PDN for security purposes.

c) Monitoring initiatives designed for the WAN shall operate within the legislated requirements for protection of personal privacy.

d) No person shall operate sniffers or other monitoring devices on the PDN without the prior authorization of the Chief Cybersecurity Officer.

e) PDN 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 PDN 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.

16. SECURITY TRAINING

a) The Chief Cybersecurity Officer shall provide training 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 and WAN Security Processes, as published on the ICTS Intranet website <https://novascotia.sharepoint.com/sites/EA/SitePages/ICT Services Standards.aspx> are supplements to this policy providing interpretation, technical standards and best practices, and guidance on implementation 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 DEPARTMENT OF SERVICE NOVA SCOTIA AND INTERNAL SERVICES (SNS-IS)

The Deputy Minister of SNS-IS is additionally accountable for the strategic development and analysis of policy, standards, and processes for information security.

CHIEF CYBERSECURITY OFFICER

The Chief Cybersecurity Officer is responsible for developing, monitoring, and proposing revisions to the WAN Security Policy and Standards in co-operation with WAN stakeholders. The Chief Cybersecurity Officer directs the implementation of the WAN Security Policy and Standards and is additionally responsible for perimeter WAN security management. The Chief Cybersecurity Officer evaluates and responds to all requests related to WAN services and security, and is responsible for investigating and responding to security incidents.

CHIEF TECHNOLOGY OFFICER

The Chief Technology Officer is responsible for operational WAN security management. The Chief Technology Officer evaluates and responds to all requests related to WAN access and ensures 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 PDN and is required to abide by the WAN Security Policy and Standards and communicate those requirements to External Entities sponsored by them.

EXTERNAL ENTITY

An External Entity is an organization having business with government, sponsored by a Client Organization and authorized by the Chief Technology Officer, 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 of the Chief Technology Officer, 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 to the Chief Cybersecurity Officer.

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.

CHIEF CYBERSECURITY OFFICER

The Cybersecurity Officer 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 Cybersecurity Officer shall monitor WAN Security Policy implementation. This responsibility includes evaluating the suitability and effectiveness of the policy and standards and taking any necessary remedial action to address identified issues. The Chief Cybersecurity Office shall also ensure that the policy and standards are formally reviewed at least every two years.

CHIEF TECHNOLOGY OFFICER

The Chief Technology Officer shall monitor compliance with the WAN Security Policy and Standards for all IT systems within their jurisdiction. The Chief Technology Officer shall notify the Chief Cybersecurity Officer 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 (Corporate Administrative Policy Manual 500, Chapter 8, Policy 8.1) 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

Executive Director, Chief Cybersecurity Officer
Cybersecurity Risk Management
Department of Service Nova Scotia and Internal Services
Internal_Services-RiskSecurity@novascotia.ca

Approval date:	***April 1, 2002***	Effective date:	***October 1, 2004***
Approved by:	***Treasury and Policy Board, Business and Technology Advisory Committee***	Administrative update:	***October 2, 2019***

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.

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.

CHIEF CYBERSECURITY OFFICER
See Accountabilities. All references to Chief Cybersecurity Officer in this document means the Chief Cybersecurity Officer or a delegate appointed by the Chief Cybersecurity Officer from time to time.

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.

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 service 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.

PERIMETER
Perimiter defense is one level of defending your network from attacks, and it works wonderfully to protect as a firewall from external attacks.

PROVINCIAL DATA NETWORK (PDN)
See Definitions

ROUTER
A network device that forwards data packets between computer networks.

SECURITY PROFILE
A minimum acceptable level of security for the WAN established by the implementation of the WAN Security Policy and Standards.

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

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.