IMT Standards **IMT Standards Oversight Committee** **Government of Alberta**	**Effective Date: 2018-10-31** **Scheduled Review: 2019-10-01** **Last Reviewed: 2018-10-01**
	Type: Technical
Standard number - A000088	
Encrypted Traffic Inspection Standard	
Category: Security **Keywords: Network, Encrypted , Network Traffic, Interception, Monitoring, Forensic**	

Description of Standard

This standard determines the approach and controls which govern the decryption and interception of IP traffic entering the GOA domain. Examination of intercepted traffic enables the protection of Government of Alberta (GoA) assets from malicious activity and malware.

This standard supports Information Security Management Directive Section 5.8.

Standard Specification

The following controls will be performed for network traffic entering into GoA networks.

1. Encrypted traffic will be decrypted and inspected based upon categories, and restricted to unknown and uncategorized domains, as well as any external host or category which may represent a risk to GoA.

2. Human examination of captured data will not occur by GoA or contracted personnel except in the event of:
    - a logged security incident and will only be performed by authorized individuals;
    - an authorized forensic investigation and will only be performed by authorized individuals;

3. Retention (storage) and human examination of captured data is only allowed in the event of a logged security incident or forensic investigation.

4. A set of technical security controls to govern the configuration, change management, auditing and access logging of the interception service must be agreed to by the Corporate Information Security Office (CISO) and the Service provider. The agreement is for the service in production and for any substantial change in the service.

Where to Apply This Standard

This standard applies to all encrypted traffic entering into the GoA internal networks.

Authority and Exceptions

Internal Use Only

Supporting Documentation

1. Information Security Management Directives (ISMD)
2. Standard Exception Form

Owner

Service Alberta, Office of the Corporate CIO, Corporate Information Security Office (CISO)

Contact

GoA IMT Standards at imt.standards@gov.ab.ca

Additional Information

Audience	Government of Alberta Information and Communications Technology (ICT) environment
Source	Service Alberta, Office of the Corporate CIO, Corporate Information Security Office (CISO)
Sensitivity	Public
Proposed Date	2018-10-01
Proposed By	Martin Dinel Executive Director Corporate Information Security Office Service Alberta Martin.dinel@gov.ab.ca ciso@gov.ab.ca (780) 427-2429

Appendix A

Types of Standards	Description
Technical Standard	These are detailed, unique standards that have developed in response to government IMT policies. Technical standards are intended to be replicable, transferable, and adaptable across ministries and other government agencies. Examples of these could include address data standards or specifications for a single identifier for transacting with government electronically.
Product Standard	An IMT product or specific technology oriented standard that facilitates the task of planning for enhancements and acquisitions within the government's broad information systems environment. As a definitive list of the numerous technologies either employed or under evaluation by Workplace Technology Services, product standards are critical in establishing conformity, interoperability and interchange-ability. Examples of these could include a government-wide standard for document, record management and database, and the list of core products for government workstations.
Process Standard	An established, mandatory business practice that supports IMT projects and existing systems to improve the outcome, diminish risks, and increase reliability. Examples could include business continuity planning processes, threat risk assessment processes, etc.
Reference Standard	An IMT industry standard (either a national or international formal or de facto standard) that has been adopted for use by the Province of Alberta. A Reference Standard may be adopted either as stand-alone or as a precursor to a customized standard or policy document. Examples could include the 1024 bit RSA standard for public key encryption.