

CGSB Standard

Electronic Records as Documentary Evidence

CGSB 72.34.05

Compliance to PIPEDA



Scope: Electronic Records As Documentary Evidence Standard

- ◆ Describes the establishment, maintenance and operation of a program for the creation, capture, storage, retrieval, delivery and disposition of electronic data in order to maximize the admissibility of electronic records as evidence in legal proceedings and to protect personal information.



Scope: Electronic Records As Documentary Evidence Standard

- ◆ This standard applies to electronic documents/record) and includes:
 - images
 - data files
 - text files
 - electronic records
 - personal information databases
 - electronic signatures
 - electronic commerce data,
 - electronic filings
 - Email
 - video files, audio files and other similar file types.



Goals of the Standard for Best Practices

- ◆ For all types of electronic records
- ◆ Focuses on integrating requirements for compliance
- ◆ Guidance and best practices for compliance
- ◆ Compliance ensures system integrity trustworthiness and reliability
- ◆ Ensures record authenticity and integrity
- ◆ Supports admissibility of electronic records
- ◆ Technology Neutral



Scope: CGSB Standard for Electronic Documents and Records

- ◆ “Electronic Records as Documentary Evidence”
 - Describes the specific level of care for developing, acquiring, implementing, maintaining and operating an electronic storage, retrieval and delivery system for electronic data
 - Provides unambiguous and clear descriptions of performance with regard to reliability, access, security, intelligibility, recoverability, non-repudiation, document/data integrity (re: content, structure and context), reproducibility and assurance of origin.



CGSB CAN 72.11-93 72-34, PIPEDA

- To comply with CAN 72.11.00, 72.34.05, PIPEDA
 - Develop a policy
 - Establish an electronic document and records management program authorized by written corporate policy
 - Confirm that the program will form part of the ‘usual and ordinary course of business’
 - Develop procedures to prove system integrity and authenticity electronic documents, records, content, personal information and metadata
 - Assign roles and responsibilities
 - Train, educate and implement
 - Audit compliance



Procedures Outline

- ◆ Purpose and/or objectives for implementation
- ◆ Authorization
- ◆ Accountabilities and Responsibilities
- ◆ Types of “records” to be stored
- ◆ Procedures for the ERM/EDMS to include each step and activity during the Information Lifecycle of Electronic Information, Personal Information and Records i.e. creation to placement in secure storage and subsequent disposition and expungement



ITI Professional Service Offerings

Legal Admissibility and Privacy

- ◆ Education and Awareness Briefings
- ◆ Requirements Assessment
- ◆ Compliance Analysis
- ◆ Policy and Procedure Write, Validate & Document
- ◆ Development/Write
- ◆ Monitor Compliance of Policies and Procedures
- ◆ System Audit
- ◆ System Certification
- ◆ Opinion Letter
- ◆ Performing Privacy Impact Assessments
- ◆ Consult with Corp. Management
- ◆ Organizational Needs Analysis
- ◆ Assess the Environment
- ◆ Certification
- ◆ Audit and Assist with Compliance
- ◆ Develop Communications Plans
- ◆ Deal with 3rd Party Partners and Contractors

Interactive Technologies - Michael Bookbinder
1 (905) 689-4838 www.itiinternational.com



Thank you

