

Information Management Policy Framework Assessment

Status	Document name of Policy	Version	Current owner	Future owner	Creation date	Approved by	Normal review process	Additional comments
C	Email Management and Usage Policy							http://www.ocio.gov.nl.ca/ocio/email/index.html
	Metadata policy							
	Paper Scanning Policy							
C	Information Management and Protection Policy							http://www.ocio.gov.nl.ca/ocio/policies/im_ip_policy.html
	eDiscovery Policy							The collection phase of e-discovery can be quite challenging, and it calls for an e-discovery policy to be created and adhered to ahead of time. The policy includes not only the standard storage and archive protocols, but will include procedures about retention period, and procedures for implementing a “legal hold” on data that might otherwise be deleted. E-discovery isn’t just ordinary backup and search. Legal counsel may for example, require access to information that isn’t traditionally contained in archives, such as data stored on individual employees’ work PCs in calendar applications, audio files, or even web browser histories. A protocol for accessing, under legal guidance, individual desktops as well as the standard archive and backup volumes must be a part of the e-discovery policy. Meta-data also needs to be preserved about each file, for example, metadata that shows when each file was most recently opened or changed.
	Records Appraisal Policy							The appraisal policy defines the methods used to determine which government records are worthy of permanent preservation.
	Information Security Policy							Information security policies provide a framework for best practice that can be followed by all employees. They help to ensure risk is minimized and that any security incidents are effectively responded to. Information security policies will also help turn staff into participants in the company’s efforts to secure its information assets, and the process of developing these policies will help to define a company’s information assets. Information security policy defines the organization’s attitude to information, and announces internally and externally that information is an asset, the property of the organization, and is to be protected from unauthorized access, modification, disclosure, and destruction.

	Records Retention and Disposition Policy							
	Vital Records Policy							http://www.im.gov.ab.ca/index.cfm?page=imtopics/vi
	Remote Access Policy (home users and partners / vendors)							
	Security and Access Policy							
	User support Policy (service level agreements)							
	Information Legal Hold Policy							The duty to preserve potentially relevant information begins when litigation or an investigation is reasonably anticipated and presents the greatest challenge for most organizations. A reasonable and defensible legal hold process is required as penalties for the failure to preserve potentially relevant information can include evidentiary sanctions, adverse rulings, and fines. The organization must not only issue, manage, and track multiple hold notices but also simultaneously ensure all relevant information is preserved. A model legal hold policy defines the roles of a Legal Hold Team, a Litigation Response Team, Data Owners (custodians), IT and Compliance. A model legal hold policy further defines the responsibilities of the teams and individuals throughout the entire legal hold business process.
C	Blackberry Usage Policy	Revision (#) 12	Colin Tibbo		22-Nov-06	Treasury Board Approval TBM 2007-300		
C	Policy for the Transmission of Personal Information via Electronic Mail and Facsimile							
C	Policy for the Protection of Personal Information in Information Technology Outsource Contracts							
	Social Networking Policy							http://www.aiim.org/infonomics/social-networking-goes-corporate.aspx