Canadian Grain Commission | Commission canadienne des grains

Canada

Canadian Grain Commission
2003-2004 Information Technology Security Review
Management Action Plan

Recommendation	Designated Authority	Individual	Action Plan Details	Timetable
#1 Align operational activities closer to GSP policies and standards	Corporate Services	CS Manager Administration	• Being developed	Ongoing
#2 Establish a co-ordinated and permanent effort to include security in all aspects of planning, budgeting and program review	Corporate Services	CS Director	• Priority for Manager of Administration	Ongoing
#3 Raise the preparedness of security within the organization	Corporate Services	CS manager of Administration	• BCP is major organizational priority	Ongoing
#4 Appointment of Departmental Security Officer	Corporate Services	CS Director	• Included as part of position responsibilities of the CS Manager of Administration	Completed
#5 Development of an IT Security Policy	Corporate Services	ITS Manager	• prepare a draft and submit to EMC for approval	Completed
#6 Development of a Departmental Security Policy	Corporate Services	CS Manager Administration	• Priority for Manager Administration	Fall 2005

#7 Development of a Departmental Classification Guidelines for data	Corporate Services	CS Manager Administration	• Plan to be developed	2006-2007
#8a Development of Procedural Documentation for various processes: - IT H/W security - S/W security - IT Security Operations - Configuration mgmt - Network Security - Teleworking - Maintenance/disposal of IT assets - Handling of IT security breaches	Corporate Services	ITS Manager / CS Manager Administration	• H/W is documented. Chatham, P.R. in transition. Ecora will complete documentation. • Security S/W is documented, (firewall, router & switched.) • IT Security operations is documented appropriately within ITS. Size of CGC & limited staff make extensive documentation not necessary. Will recommend usage of ID tags within ITS. • Configuration mgmt to be done by Ecora. • Network security is documented appropriately considering size, complexity and track record of CGC. • Maintenance / disposal of ITS assets is done according to CGC	Completed. Ecora installed early 2005.

			policies. • Teleworking policy will be developed. • The CIO will be informed in writing of significant security breaches.	
#8b Review and revise existing policies to agree with the Procedural Documentation	Corporate Services	ITS Manager	• Revamp Inet and e-mail policies	Completed
#9a Completion of the Business Continuity Plan (BCP) and the Business Disaster Recovery Plan (BDRP)	Corporate Services	CS Manager Administration	• Prepare BCP draft and review with Vancouver regional office • Roll out BCP to all other regional offices • Initiate BDRP	Fiscal years 2005-2006 and 2006-2007
#9b Prepare an inventory list of CGC vital assets and critical files	Corporate Services	CS Manager Administration	• Part of BCP	Fiscal years 2005-2006 and 2006-2007
#10 Development of Statements of Sensitivity for existing and new systems be included as part of the System Development Methodology (SDM)	Corporate Services	ITS Manager	• To be done in consultation with the application team	Fiscal year 2005-2006
#11 Appointment of an IT Security Officer	Corporate Services	CS Director	• Identify and recommend to EMC	Completed

			for approval	
#12a Perform Threat Risk Assessments (TRA) with other IT security inspections	Corporate Services	ITS Manager	• TRAs are done as per item #14 (done when necessary for PID)	Completed
#12b Perform Network TRA's and review Tier 3 technical security measures	Corporate Services	ITS Manager	• General IT security reviews should be done every 5 years. Based on track record and experience do not agree detailed technical (Tier 3) security assessment is necessary at this time..	Completed
#13a Enhance SDM to include security and privacy requirements	Corporate Services	ITS Manager	• Security requirements are included now in the SDM & privacy concerns are being noted. We will formalize the process once item #7 is completed.	Completed
#13b SDM to be applied to all new applications	Corporate Services	ITS Manager	• We are requiring all S/W be developed according to the SDM we use.	Completed
#14 Implement a Risk	Corporate Services	ITS Manager	• An informal process is	Completed

Management Framework for IT development			followed & the CGC Project Mgmt process will include risk/mgmt where applicable. Recommendation for a formal process to use in IT is unnecessary. • Not viewed as a high priority at this time	
#15 Process or store classified documentation on a stand alone computer	Corporate Services	ITS Manager	• To be addressed, after item #7 has been resolved.	2006-2007
#16 Install a secure fax machine for classified data	Executive	Chief Operating Officer	• CGC has access to AAFC secure fax in CGC headquarters	Completed
#17 Perform IT awareness sessions to staff	Corporate Services	ITS Manager	• Identify opportunities to raise staff awareness (e.g. CGC newsletter articles)	Ongoing
#18 Formalize requirements or interoperability standards for procurement of hardware and software products	Corporate Services	ITS Manager	• Standards are informal now. However, desktop policy will address this recommendation. We have begun movement towards stricter enforcement of standards through	Completed

			modified reporting relationships for regional staff, improved procurement process, remote monitoring S/W, new H/W and policy development. • Testing is complete • Policy still to be developed	Policy to be developed in Fiscal Year 2005-2006
#19 Document network configuration and store a copy off-site	Corporate Services	ITS Manager		Completed
#20 Document and implement procedures for remote access	Corporate Services	ITS Manager	• Prohibit use of modems within the network perimeter	Completed
#21 Review current staffing authorities with respect to administrative rights to classified and sensitive data	Corporate Services	ITS Manager	• We have some authorities in place now. (e.g. IT regional staff do not have admin rights to the national network, access to e-mail logs). IT takes what are felt to be reasonable steps regarding access and admin privileges. IT allocates resources to critical systems with	Completed

			back-up capacity in mind. Separation of duties is done where security is a concern. (e.g. Finance) • Will continue to review periodically	
#22 Consider procuring additional security features for laptops and stored data	Corporate Services	ITS Manager	• Not viewed as a high priority at this time • To be reviewed at a later date	Completed ongoing requirement in managing the network.
#23 Develop policies to assist in managing emerging threats resulting from new technologies	Corporate Services	ITS Manager	• Enhance communication to all employees • CGC linked to OCIPEP	Completed
#24 Development of a formal approach for detecting, analyzing and responding to security related events	Corporate Services	ITS Manager	• Not viewed as a high priority at this time • To be reviewed at a later date	Fiscal year 2008-2009
#25 Review the current situation with respect to the risk related water leakage on servers	Corporate Services	ITS Manager	• Contact the facilities officier to investigate the issue and provide a recommendation • No action was deemed necessary	Completed