



APPENDIX E
28 February 2008

**Ottawa Congress Centre Redevelopment Program
Procurement Policy**

ACCESS SECURITY AND DOCUMENT MANAGEMENT POLICY

Objective

To ensure the integrity of the OCC Redevelopment Project (including the pre-RFQ, pre-RFP and contracting periods), all project information designated as CONFIDENTIAL (by the Development Advisor and/or by Ottawa Congress Centre) must be safeguarded in an appropriate manner. Appropriateness in this context is measured by the achievement of maximum assurance that no party to the bidding for the OCC facility development contract has unauthorized access to relevant data or information that could give such party any preference or advantage relative to any other party.

Responsibility and Authority

The Development Advisor is responsible for achieving and maintaining the project's access, security and document management objective. The Development Advisor will implement the access, security and document management (ASDM) program approved by the OCC President.

The Development Advisor will:

1. ensure that all project personnel who develop or have access to CONFIDENTIAL information have been briefed on their security responsibilities
2. maintain an active security awareness program
3. ensure that only project personnel, OCC officials, OCC directors and government officials with a "need to know" have access to CONFIDENTIAL information
4. on the understanding that access to CONFIDENTIAL project information is restricted to authorized persons with a need to know, approve the physical access security and document management solutions implemented at each project site.
5. approve the assignment of LAN/WAN systems and network administrators responsible for the integrity of electronically stored project data and documents at the various sites

6. approve the electronic access (password) security solutions and document management systems implemented at each project site
7. ensure that all CONFIDENTIAL project data and documents are protected and handled in accordance with the provisions of the ASDM
8. ensure that the OCC President is promptly notified of any breach or compromise of security
9. investigate breaches of security or instances of compromise and report findings and recommendations to the OCC President
10. initially, as a condition of participation on the project and thereafter, periodically or at random, audit each project site to ensure compliance to the ASDM program requirements.

Site Security Officers

Because the project team is deployed at multiple sites, each site will designate a Site Security Officer (SSO) who, for the purposes of the ASDM program, ensures compliance to the program for that site.

SSO's shall report to the Development Advisor the security status of their respective sites. In the normal course, such reports will take the form of an ASDM program checklist. ASDM incident reports will be submitted to the Development Advisor in real time for his consideration and action. The SSO will provide a written report monthly or when any breach of the policy is noted to the Development Advisor.

Safeguarding and Handling CONFIDENTIAL Project Information

Access to CONFIDENTIAL project data and information must be limited to persons who have a need to know. Such persons will be identified:

1. in the case of project personnel (including consultants) , by the Development Advisor
2. in the case of OCC officials, by the OCC President
3. in the case of OCC directors, by the OCC Expansion Committee, taking account of the OCC President's recommendations
4. in the case of government officials, the main point of contact federally, provincially and municipally

Marking Documents

All CONFIDENTIAL information shall have the following security warning on both the front cover and title page:

“This document contains CONFIDENTIAL information affecting the OCC Redevelopment Project. It has been produced by (originator’s name) and is to be safeguarded, handled and transported in accordance with the provisions of the Project Security Instructions. Release of this document, or any information contained herein, to any person not authorized to receive it is prohibited and may result in dismissal or termination or other appropriate action.”

Copies of all CONFIDENTIAL information shall include the word “CONFIDENTIAL” in the upper right corner of the face of each page of a document. Documents that only become classified CONFIDENTIAL when completed should be marked “CONFIDENTIAL (when completed)” and be treated in the same manner as though completed. Control copies of CONFIDENTIAL project documents must show the copy number on the face of each copy and be accompanied by an up-to-date distribution list. In the case of electronically stored project documents, the same marking requirements apply preferably with the ability to display the CONFIDENTIAL mark in both eye-readable and machine-readable forms. Removable storage material (diskettes, CD’s, etc.) must bear standard labels indicating the CONFIDENTIAL classification.

Document Control and Storage

The OCC Redevelopment project management office and each project site will maintain adequate facilities and services for receiving, distributing and storing CONFIDENTIAL project information. A record shall be kept of the dates, names and transactions of all CONFIDENTIAL information including:

1. receipt at the site
2. distribution within the site
3. origination within the site
4. reproduction within the site
5. destruction within the site
6. transmittal outside the site

When not in use, CONFIDENTIAL project information shall be stored in a locked container. The adequacy of the container options will be determined by the Development

Advisor. Keys (conventional, card, combination, etc., used to open and secure containers) shall themselves be safeguarded. When a key is issued, the recipient's name will be recorded by the SSO. Assigned keys are subject to change at the discretion of the SSO commensurate with the perceived security risk. When a container has been compromised, the key must be changed immediately.

Special care must be taken to protect against disclosure or unauthorized access to CONFIDENTIAL project information when in use outside of the approved container. Specific points to observe are:

1. do not leave CONFIDENTIAL information unattended
2. ensure that CONFIDENTIAL information cannot be viewed, or discussion of it overheard, by unauthorized persons or persons without a need to know
3. maintain a "clean desk" policy after normal business hours and ensure that cleaning and maintenance staff are appropriately supervised at each project site
4. secure facsimile machines must be used when transmitting/receiving CONFIDENTIAL project information
5. email must not be used to transmit CONFIDENTIAL documents but these documents can be obtained by authorized team members through www.gbassociates.ca. Exceptions to this requirement necessitate explicit written approval of the Development Advisor
6. project personnel authorized to download or take CONFIDENTIAL project information out of the project office or any of its sites for off-site work must ensure that all ASDM directives are followed. Document tracking and control should be at the highest standards to ensure integrity of the procurement process. Hard copies of controlled documents must be signed in and out through the SSO.
7. recording devices or cameras are not allowed on project sites except in a secured area.
8. no wall (flip) charts or chalk board displays of CONFIDENTIAL information can be visible from outside a project site at any time nor can any such display remain during non-working hours.

Document Copying/Printing

Special precautions must be taken with the use of photocopy machines and printers. Notices concerning the proper procedures for reproduction of CONFIDENTIAL project information shall be placed in an obvious location close to each machine. Care should be taken to ensure that original documents are not left in the machine and that all copies, including waste, are removed. Reproduction of CONFIDENTIAL project information shall be documented as per the controls put in place and authorized by the SSO.