Controlled Goods Security Plan

Designated Controlled Goods and Technology Areas at the University of Ottawa

Office of Risk Management
1 Nicholas, Suite 840
Ottawa ON K1N 6N5

Faculty of Social Sciences
120 University
Ottawa ON K1N 6N5

Faculty of Medicine
451 Smyth
Ottawa ON K1H 8M5

Table of Contents

1. What is the Controlled Goods Program

The Controlled Goods Program (CGP) is a registration and compliance program, mandated by the Defense Production Act (DPA) of Canada that regulates access, examination, possession or transfer of controlled goods. The University's CGP mandate is achieving and maintaining compliance with the requirements in safeguarding controlled goods in Canada and supporting Canada's export control regime.

The Office of Risk Management (ORM) will help you determine if you need to undergo a security assessment through the Controlled Goods Program and will perform the necessary steps to complete that registration on your behalf.

The program is responsible for:

- registering the University and individuals who examine, possess or transfer controlled goods performing security assessments;
- processing exemption from registration applications;
- conducting inspections and ensuring compliance with controlled goods legislation;
- investigating security breaches; and
- working with law enforcement agencies for enforcement-related actions of the Defense Production Act.

2. Why is the University of Ottawa registered under the CGP?

The University of Ottawa is registered under the Federal Government Controlled Goods Program, a security program managed by Public Services and Procurement Canada. As per many Canadian universities, it is possible that the University of Ottawa will need to examine, possess or transfer controlled goods or technology within the limitations of research projects. Therefore registration is mandatory.

As conditions of its registration under the Controlled Goods Directorate (CGD), the University of Ottawa established this controlled goods security plan. The purpose of this security plan is to prevent unauthorized individuals from accessing controlled goods and to ensure compliance with the Controlled Goods Regulation as well as University guidelines and policies.

3. Obligations and implications

The University of Ottawa, as with all other registered institutions, must be represented by an authorized individual. Michael Histed, PhD, director of the Office of Risk Management, acts as the University's authorized individual. All registered institutions must appoint at least one designated official, who will have administrative responsibilities for the CGP. Michael Histed and Pascal Simard, Assistant Director, are the designated officials for the CGP at the University of Ottawa.

All University of Ottawa employees, temporary workers, students and visitors who wish to access or make use of controlled goods or technology must apply to the Office of Risk Management for authorization as described in section 5 of this security plan.

4. Accountability and responsibilities

4.1. Authorized individual

The authorized individual, on behalf of the applicant, will be responsible for:

- Ensuring that a designated official is appointed for each place of business in Canada where controlled goods or technology are kept; and

- Approving by their signature any changes in any of the information contained in the application for registration.

University of Ottawa authorized individual:

Michael Histed
Director, Office of Risk Management
1 Nicholas, Suite 840
Ottawa ON K1N 7B7
Phone: 613-562-5273
Fax: 613-789-5711
Email: michael.histed@uOttawa.ca

4.2. Designated official

The designated official (DO) is a liaison between the University of Ottawa and the Controlled Goods Directorate (CGD). The role of the DO is as follows:

- Conduct security assessments in accordance with Section 15 of the CGR with the consent of the individual concerned and evaluate applications received for authorization for full-time employees and temporary workers who are not exempted from registration and are Canadian citizens to access CG/CT
- Submit applications to the CGD on behalf of foreign temporary workers who are exempt from registration and visitors to the University as well as conduct a preliminary security evaluation of workers who wish to access CG/CT
- Establish and maintain a record of controlled goods technology
- Establish and implement a security plan
- Provide training programs and security briefings on the secure handling of controlled goods or technology
- Advise the CGD of any security breaches involving controlled goods or technology

University of Ottawa designated official:

Pascal Simard
Assistant Director - Environmental Management
Office of Risk Management
1 Nicholas, Suite 840

Ottawa ON K1N 7B7
Phone: 613-562-5800 extension 2487
Fax: 613-789-5711
Email: psimar2@uOttawa.ca

4.3. Authorization committee

An Ad Hoc authorization committee is put together on an as needed basis to assists the designated official in implementing security plans and evaluating applications for authorization for access to CG/CT. A confidentiality agreement must be signed by each member of the authorization committee; members are not to discuss information with unauthorized individuals. Members of the authorization committee are selected by the designated official from relevant departments at the University of Ottawa.

4.3.1 Members of authorization committee

- Designated official
- Associate vice-president, Research
- Representative, Human Resources Service
- Assistant director, Protection Services
- Assistant director, Environmental Management, Office of Risk Management

4.3.2 Responsibilities of authorization committee

- Recommend to the designated official any elements of the security plan that need modification
- Review and examine the handling of CG/CT by authorized individuals
- Notify the designated official of a security breach, adverse event or any violation of the regulations or policies relevant to the University of Ottawa's CGP
- Arrange a meeting with the designated official for revoking the authorization of any individual in the case of a security breach
- Attend periodic meetings called by the designated official for the purpose of administering the University of Ottawa's CGP

5. Security standard and procedures for controlled goods and technology (CG/CT)

5.1. Security plan related to CG/CT

The purpose of this security plan is to prevent unauthorized individuals from accessing CG/CT and to ensure compliance with the Controlled Goods Regulation as well as University guidelines and policies.

The security plan for the Controlled Goods Program at the University of Ottawa is under the responsibility of the Office of Risk Management. The security plan is updated as new CG/CT is made available to the University of Ottawa or in accordance with any new CGD requirements.

The Office of Risk Management, Protection Services and the Research department of the University of Ottawa are responsible for the implementation and maintenance of the plan.

5.2. Security assessment procedures

Depending on the status of the applicant wishing to examine, possess or transfer controlled goods or technology, different application forms must be completed, as set out in the *Controlled Goods Regulations*. In some case, however, the applicant may be exempt from a security assessment.

The DO may approve an application for authorization by signing an agreement of authorization with the applicant. Authorization is not transferable.

The DO may suspend or withdraw authorization to access CG/CT if security procedures are not followed.

The designated official may reject the application for authorization by sending a notice to the applicant indicating the reasons access to CG/CT is being denied.

An individual who is the subject of a security assessment must inform the DO without delay of any change in information.

5.2.1 Identify the required security assessment

To determine the appropriate security assessment required, an applicant must determine their status at the University of Ottawa, as defined by the *Controlled Goods Regulations*. The following definitions are presented to assist applicants in choosing the correct forms. If you require assistance with this process, please contact the designated official at the Office of Risk Management.

Status	Definition	Example	Security assessment process
Employee, director, officer	A person employed by the University of Ottawa to perform duties for remuneration that is a Canadian citizen or a permanent resident of Canada	• Faculty personnel • Support staff • Contractual worker who is an employee of the University of Ottawa • Student working for a faculty that is from a Canadian University	Section 5.2.3
Temporary worker	An officer, director or employee of the University of Ottawa **who is not** (a) a Canadian citizen ordinarily resident in Canada **or** (b) a permanent resident ordinarily residing in Canada	• Student from a non-Canadian University working for a faculty	Section 5.2.4
Visitor	An individual **who is not an** officer, director or employee the University of Ottawa **and who is not** (a) a Canadian citizen ordinarily residing in Canada **or** (b) a permanent resident ordinarily residing in Canada	• A professor from a non-Canadian University visiting a faculty	Section 5.2.5

5.2.2 Exemptions

5.2.2.1 Individual registered under the *International Traffic in Arms Regulations* (ITAR)

Specifically with respect to temporary workers or visitors who are officers, directors or employees of persons registered under ITAR, an individual is exempt from registration from CGD from the day the individual provides the University of Ottawa with:

- Evidence of the individual's status as director, officer or employee of a person registered under ITAR,
- Evidence of the registration and eligibility of the ITAR-registered person and
- Evidence of the eligibility of the individual under ITAR.

Eligible means an individual not debarred or suspended under ITAR and therefore able to participate directly or indirectly, under ITAR, in the export or import of defense-related articles, including technical data furnishing defense services for which a license or approval is required.

5.2.2.2 Other exempt persons

The following classes of persons, including as a visitor or temporary worker, are also exempt from registration with CGD:

- Canadian public officers, as defined in Section 117.07 (2) the Canadian *Criminal Code*
- Elected or appointed officials of Canada's federal or provincial governments
- Members of a "visiting force," as defined in section 2 of the *Visiting Forces Act* present in Canada in connection with official duties, including civilian personnel designated under section 4 of the Act as a component of the visiting force
- Officers, employees or elected or appointed officials of the United States federal, state or territorial governments who are acting in good faith in the course of their duties and employment

These persons must provide evidence to the DO that they are members of an exempt class of persons (i.e., legal name of person, name of government department of agency, copy of identification card) and the time and date of their visit.

5.2.3. Security assessment for employees, directors, officers

The DO conducts a security assessment of each officer, director and employee who requires, in the course of their duties, access (examination, possession or transfer) to controlled goods or technology if these individuals are either a Canadian citizen ordinarily residing in Canada or a permanent resident of Canada. The security assessment takes into account the following details during the five years prior to request for such assessment:

- personal references
- criminal record
- place(s) of residence
- employment history
- education history

Authorization to examine, possess or use controlled goods is the exclusive decision of the designated official. The DO may decide to ask the authorization committee to assist in gathering or verifying information for the security assessment. See sections below for additional information.

The security assessment process is the same for every applicant, regardless of whether it is for full or partial access to CG/CT.

5.2.3.1 The applicant has a valid Government of Canada clearance

If an officer, employee or director subject to a security assessment under the Controlled Goods Directorate has a valid security clearance granted by the Government of Canada at the Secret level or higher, this is considered sufficient for the purpose of a security assessment under the CGD. Consequently, the DO will not have to conduct a CGD security assessment on these individuals.

The applicant must complete the Consent to use a Government of Canada Security Clearance form of the Controlled Goods Directorate.

The original forms and required documentation must be submitted to the DO with the mention PERSONNEL AND CONFIDENTIAL on the envelope.

5.2.3.2 The applicant does not have a valid Government of Canada clearance

If the applicant does not have a valid Government of Canada Clearance, the individual must complete the Security Assessment Application – Owner, Authorized Individual, Designated Official, Officer, Director, Employee form of the Controlled Goods Directorate.

The original forms and required documentation must be submitted to the DO with the mention PERSONNEL AND CONFIDENTIAL on the envelope.

5.2.3.3 Documenting the security assessment

The DO must document the security assessment using the Security Assessment Summary by Designated Official Conducting a Security Assessment of an Employee, Director, Officer, or Authorized Individual of the Controlled Goods Directorate Policy Guideline on Security Assessment by Designated Officials.

5.2.3.4. Security assessment decision

The DO must inform the applicant of the decision on the security assessment. If the **assessment if positive,** the DO completes the Notice of Security Assessment and Authorization (Positive Assessment) of the Controlled Goods Directorate Policy Guideline on Security Assessment by Designated Officials.

If the applicant is **negatively assessed**, the DO completes the Notice of Security Assessment (Negative Assessment) of the Controlled Goods Directorate Policy Guideline on Security Assessment by Designated Officials.

5.2.4. Authorization procedure for temporary workers

A temporary worker is eligible for an exemption from registration with CGD only if the University of Ottawa submits an application on their behalf to the Minister of Public Works and Government Services Canada (PWGSC) through the Controlled Goods Directorate (CGD) and the temporary worker consents to a security assessment.

To conduct the assessment, the DO must complete and submit an application form and required evidence to the CGD, which will perform the security assessment of the individual.

The DO submits an application to the CGD for an exemption with respect to each temporary worker, on

a form supplied by the CGD (Application for Exemption Form Registration). Similarly, the temporary worker must consent to a security assessment on a form supplied by the CGD (Security Assessment Application Form) and provide the information required.

5.2.5. Authorization Procedure for Visitors

The Designated Official must complete an Application for Exemption Form Registration (Visitor) for exempt visitors and submit it to the Controlled Goods Directorate (CGD), which will conduct a security assessment of the individual.

Visitors who have not received registration exemption from the Controlled Goods Directorate are to be informed that they are not authorized to examine, possess or transfer controlled goods during the course of their visit.

5.3. Security procedures to receive, keep, transfer and dispose of controlled goods or technology

5.3.1 Responsibilities of principal investigators

The following processes and procedures are to be employed by the principal investigators (PIs) and their team members.

- PIs must cooperate in providing evidence of the individual status of their team members to the Office of Risk Management in the case of access to controlled goods or technology.

- Depending on the status of PIs and their team members, the Office of Risk Management will conduct a security assessment on the individuals who possess or transfer controlled Goods or technology in accordance with Section 15 of the *Controlled Good Regulations*.

- PIs are responsible for informing members of their team who possess or transfer CG/CT of the procedures for possessing and transferring CG/CT and the requirement to review this Security Plan and CGD newsletters on an annual basis.

- PIs must inform the designated official at the Office of Risk Management of any visitor who will have access to CG/CT.

- PIs must advise team members not to discuss matters related to controlled goods with other employees or individuals who have not been completed a security assessment for Controlled Goods Program.

- PIs must inform the designated official at the Office of Risk Management in the case of any loss or other breach.

5.3.2. Procedures for receipt of controlled goods

The authorized faculty health, safety and risk managers (HSRMs), or designates, at the University of Ottawa are in charge of updating the chemical inventory, keeping a record of receipt of controlled

goods and technology and preparing and filing a semi-annual report to the designated official at the Office of Risk Management.

The report must contain:

- The date of purchase of CG/CT
- The name of the CG/CT supplier
- The CG/CT supplier contact name

5.3.3 Designated areas of controlled goods and technology

Controlled goods and technology are to be kept in a locked location in order to prevent access by unauthorized personnel. The designated controlled areas are equipped with an electronic card reader or a lock, restricting access to authorized individuals.

Responsibility for access keys is determined by the designated official based on the authorized individuals' status.

The name of registered individuals, time and date of access to the controlled goods or technology in the designated area is to be recorded and submitted to the designated official with the semi-annual CG/CT report.

The designated areas are monitored by live security cameras.

5.3.4 Use of controlled goods

In case of physical contact with controlled goods or technology, the following information must be recorded in the log or access sheet: name, employee or student number, date, use and signature. The log is kept in the same cabinet as the controlled goods or technology is kept.

5.3.5. Procedures for transfer of controlled goods

The PI must inform the designated official at the Office of Risk Management before transferring controlled goods or technology. The PI must record the date of transfer as well as the location and name of the receiver and submit the information to the designated official. The designated official must record all transfer information and retain all transfer records.

5.3.6. Procedures for disposal of controlled goods

The PI must inform the designated official at the Office of Risk Management of his intention to dispose or destroy the controlled goods or technology. The designated official will manage the disposal process and send a special disposal request to the hazardous material technical services manager. The request will contain a list of chemicals or technology that need to be transferred, destroyed and disposed, including the procedures, specific to each goods, for their destruction and disposal. The request must clearly indicate the product name, CAS number, barcode number and lab location of the chemicals.

The designated official is responsible for supervising the transfer in the hazardous waste room, listing and recording the date of transfer, product name, CAS number, barcode number and destruction protocols in the **Controlled Goods Program** document folder.

The designated official must supervise the process of mixing and destroying the controlled goods to ensure it is completed. The hazardous waste management company then disposes of the goods as required by provincial legislations.

The Controlled Goods Program document folder must be checked periodically by the designated official, who is also responsible for submitting the list of chemicals to the hazardous waste management company in charge of disposing of the identified chemicals at the University of Ottawa. The designated official must contact only individuals at the hazardous waste management company who hold a valid security clearance issued either by the CGD or the University of Ottawa's Office of Risk Management.

Once the chemicals listed in are disposed of, the hazardous waste management company advises the designated official by email that the chemicals have been disposed. The email must indicate the disposal date of the chemicals listed. The designated official must maintain records of destruction. All transfer information must be documented in keeping with section 8 of this security plan.

6. Controlled goods and technology training and briefing

All persons who have access to CG/CT will review this security plan and receive basic training on the secure handling of controlled goods and technology annually from the designated official. The training program and security plan must meet the regulatory criteria.

Individuals with exempt status will receive briefing from the designated official on the specific security plan required for the controlled goods or technology to which the individuals will have access.

6.1. Training program

Officers, administrators, researchers, employees and temporary workers who are directly or indirectly involved with controlled goods or technology will receive training from the designated official at the Office of Risk Management.

The goal of the annual training is to ensure the individual is knowledgeable on the security plan and has written documentation on the security plan for controlled goods or technology.

6.1.1. Elements to be covered during the training program

- Responsibilities and reporting obligations
- Security breaches
- Security briefing, if applicable
- Location of controlled goods and logbook that contains the date and the name and signature of authorized person
- Record keeping
- Contact information

6.2. Briefing session

Individuals with exempt status receive briefing on the specific security plan for controlled goods or technology at the University of Ottawa by the designated official.

6.2.1. Elements to be covered during the security briefing

- Access requirements and limits
- Location of the controlled goods and logbook that contains the date and name and signature of the exempt individual and the name of the security official who conducted the security briefing
- Requirement for semi-annual report

6.2.2. Elements to be covered by DO during security briefing of visitors exempt from registration by the Controlled Goods Directorate

- Any limitations imposed on the exemption certificate or otherwise imposed by the University of Ottawa

7. Security breaches

7.1 Identifying security breaches

Security breaches include destruction, modification, removal or disclosure of controlled goods or technology. Below is a list of examples of security breaches:

- Loss of a controlled good (theft or disappearance)
- Unauthorized access to a controlled good
- Willful or deliberate damage of a controlled good
- Willful or deliberate tampering with a controlled good
- Unauthorized persons examining controlled goods or technology
- Transfer of a controlled good (including information) to an unauthorized person

Identification of security breaches is the responsibility of all authorized personnel, who must advise the DO of the breach.

The DO must advise the CGD, without delay, of any security breach. CGD can be reached as indicated below:

- Telephone: 1-866-368-4646
- Fax: 613-948-1722
- Email: dmc-cgd@tpsgc-pwgsc.gc.ca
- By courier: Director, Controlled Goods Directorate
  2745 Iris Street, 3rd Floor
- c/o PWGSC Central Mail Room
  Place du Portage, Phase III 0B3
  11 Laurier Street, Gatineau
  Ottawa ON K1A 0S5
- By mail: Controlled Goods Directorate
  PWGSC
  2745 Iris Street, 3rd Floor
  Ottawa ON K1A 0S5

If the breach is of a criminal nature (such as theft), the DO will report the matter to the appropriate police body or agency and the offender may be subject to conviction under the *Criminal Code*.

7.2 Investigating security breaches

Security breaches must be fully investigated by the registered person's security organization, and corrective action must be taken to prevent any recurrence. The investigation will be led by a member of the authorization committee.

The following elements will be investigated:

- Who was involved?
- What controlled goods were involved?
- Where did the breach take place?
- When did the breach occur?
- Why did it occur?
- How did it occur?

The investigation is to be documented in a report, which must lay out corrective measures to be taken in order to ensure that similar security breaches do not occur again in the future.

8. Records management

The DO is responsible for keeping and maintaining records during the period of registration and for five years following the date of authorized access to controlled goods or technology unless otherwise indicated below:

- Controlled Goods Program documents are kept in a separate locked cabinet at the Office of Risk Management and/or in a restricted file on the server. Electronic documents must be password protected and/or encrypted.
- Logbooks must be kept in the locked cabinets in the laboratory working area or close to the area where work with controlled goods or technology is done.
- The evidence referred to in subsection 16(2) of the CGR for ITAR-exempt individuals and any other foreign visitor are kept for a *period of two years after the day on which the individual ceased to have access to the controlled goods*.
- A record must be kept of the description of any controlled goods or technology received, the date of their receipt and the identity and address of the person who transferred them to the University.
- Transfer logs of controlled goods or technology must be kept.
- A description of the manner and date of the disposition of controlled goods must be recorded.
- Records of all security breach investigations must be retained.

Any obsolete records are to be destroyed. Electronic devices of authorized personnel are to be cleaned or reformatted by IT personnel before they are disposed of.