DALHOUSIE UNIVERSITY		
Inspiring Minds	Subject: Controlled Goods and Technologies	Date Issu
	Title: **Controlled Goods Policy**	*Date Effective:* April 1, 2013
	Issued by: Martha Crago, Vice President Research	*Approved by:* Tom Traves, President

A. Background and Purpose

Dalhousie University is registered with the Controlled Goods Program (CGP), a Federal Government program administered by the Controlled Goods Directorate (CGD) under the *Defence Production Act* and the Controlled Goods Regulations. The CGP is intended to safeguard controlled goods and controlled technologies within Canada and to prevent controlled goods and/or technologies from being accessed by unauthorized persons.

This policy outlines university community members' obligations and procedures in relation to [illegible] technologies in accordance with CGP requirements.

B. Application

This Policy applies to all individuals and organizations engaged in research, teaching and other [illegible] University who seek access or have been granted access to a controlled good and/or technology undertaking through the University.

C. Definitions

1. In this Policy:

   a. "Access" means to examine, possess or transfer controlled goods and/or controlled technologies.

      i. "Examine" means to consider in detail or subject to an analysis in order to discover essential features or meaning.

      ii. "Possess" means either actual possession, where the person has direct physical control over a controlled good and/or controlled technology at a given time, or constructive possession, where the person has the power and the intention at a given time to exercise control over a controlled good and/or controlled technology either directly or through another person(s).

      iii. "Transfer" means to dispose of a controlled good and/or controlled technology or disclose its content in any manner.

   b. "Controlled Goods and/or Controlled Technologies" mean those goods and technologies listed in the schedule to the *Defence Production Act*. They include, but are not limited to,

      i. Group 2 – Munitions: automatic weapons, firearms, ammunition, weapons sights, bombs, planes, tanks, missiles, chemicals, explosives and related equipment and accessories.

      ii. Group 5 - Strategic goods: global navigation satellite systems, ground control stations, nuclear weapon design and testing equipment.

      iii. Group 6 - Missile technology: rocket systems, unmanned air vehicle systems, propulsion components and equipment.

   For further clarity, the technology required to develop, produce, support or use a controlled good is also controlled. This includes technical data, such as blueprints, formulas, engineering designs or models, and technical assistance, such as instructions, training and working knowledge related to controlled goods.

   c. "Designated Official" means the individual employed or appointed by Dalhousie University who, subject to approval of a security assessment by the CGD, is

d. "Member of the University Community" means any individual who is engaged in research, teaching or other activity at, on behalf of, in connection with or under the auspices of the University.

e. "Registered Person" means a person (an individual, organization or corporation) [illegible] with Controlled Goods and/or Controlled Technologies and who is registered with the CGD.

f. "Security Assessment" means an assessment carried out by the Designated Official which determines the reliability, trustworthiness and honesty of an individual and the risk of that individual mishandling Controlled Goods and/or Controlled Technologies. A security assessment will typically include a review of personal references, criminal history, places of residence and employment and educational histories for the five years immediately preceding the date of the applicant's consent to undergo the Security Assessment.

g. "Security Breach" includes, but is not limited to:

i. loss of a Controlled Good and/or Controlled Technology;

ii. unauthorized Access to a Controlled Good and/or Controlled Technology;

iii. appearance of damage to or tampering with a Controlled Good and/or Controlled Technology; or

iv. transfer of a Controlled Good and/or Controlled Technology to an unauthorized person.

D. Policy

1. Any member of the University Community or any other person or organization who wishes Access to a Controlled Good and/or Controlled Technology in connection with an activity conducted under the auspices of the University is required to follow the process set out in the Procedures and to follow any directions given by the Designated Official in connection with this Policy in order to ensure that the University's obligations under the CGP are met.

2. When a Member of the University Community believes that a Security Breach has occurred, he or she is under a positive obligation to immediately report the matter to the Designated Official.

3. All Members of the University Community are expected to cooperate in any duly authorized inspection or audit activities of the CGD.

4. Failure to follow this Policy may result in prosecution under the *Defence Production Act* and possible disciplinary action in accordance with applicable disciplinary procedures.

E. Administrative Structure

1. Authority: This Policy falls under the authority of the Vice-President Research.

2. Designated Official: The Designated Official is the Legal Advisor, Research Services. He or she carries out duties prescribed by the Controlled Goods Regulations and the *Defence Production Act* which include, but are not limited to:

   a. Assisting individuals to determine whether a good or technology falls within the scope of this Policy;

   b. Ensuring all individuals and organizations who may have access to Controlled Goods and/or Controlled Technology in the University's possession have undergone required security clearances;

   c. Implementing a security plan in relation to Controlled Goods and/or Controlled Technologies at the University. The security plan will include, but is not limited to:

      i. Establishing security processes to control Access to Controlled Goods and/or Controlled Technologies;

      ii. Identifying those responsible for the security of Controlled Goods and/or Controlled Technologies along with a description of their specific responsibilities;

      iii. Establishing procedures for reporting and investigating Security Breaches in relation to Controlled Goods and/or Controlled Technologies.

   d. Providing security briefings and training programs regarding Controlled Goods and/or Controlled Technologies, and

   e. Keeping appropriate records regarding all aspects of the Designated Official's duties under this Policy.

3. Record Keeping: Records regarding all aspects of this Policy, including supporting documentation, will be kept separate from all other University records and will be maintained and stored securely and confidentially under the care and control of the Designated Official.

F. Procedures

1. Access to Controlled Goods and/or Controlled Technologies

a. The Designated Official is responsible for determining whether any individual may Access a Controlled Good and/or Controlled Technology and the circumstances under which Access can occur.

b. Any person who wishes to Access a Controlled Good and/or Controlled Technology at the University or in connection with an activity undertaken under the auspices of the University must disclose this information in writing to the Designated Official at least 2 months before they intend to Access the Controlled Good and/or Controlled Technology.

c. Each member of the University Community who intends to Access a Controlled Good and/or Controlled Technology must consent to a Security Assessment by the Designated Official. Authority to Access a Controlled Good and/or Controlled Technology will be granted by the Designated Official only to those individuals whose Security Assessment was deemed satisfactory.

d. The Designated Official may define the terms under which Access is granted to [illegible] to ensure compliance with the EDR and compliance with any other regulatory or contractual obligation associated with the research or activity with which the Access is granted.

e. Participation in a training or security briefing as described in section F.2 is mandatory for all individuals seeking Access.

f. The process for determining Access by persons who are not members of the University Community depends on the status of the person seeking such Access. The Designated Official will advise such person of the details of that process upon being notified of their intent to Access Controlled Goods and/or Controlled Technologies.

2. Training Programs and Security Briefings

a. The Designated Official or designate will provide mandatory training programs or security briefings, as appropriate, to every individual who is authorized to Access a Controlled Good and/or Controlled Technology at the University prior to that person having such Access.

b. The Designated Official will review the content of training programs and security briefings periodically to ensure they continue to meet the security needs for safeguarding the specific Controlled Goods and/or Controlled Technologies and to reflect any regulatory or legislative changes.

3. Security Breaches

a. Any known or suspected Security Breach in relation to this Policy must be reported immediately to the Designated Official and Security Services. Upon receipt of this report, the Designated Official must in turn report the Security Breach to the CGD.

b. Corrective measures to a Security Breach must be implemented by members of the University Community as directed by the Designated Official without delay.