(Example)

CONTROL PROCEDURES

FOR

UNCLASSIFIED TECHNICAL DATA

DISCLOSING MILITARILY CRITICAL

TECHNOLOGY

TITLE: Unclassified Technical Data Control Procedures

PROC. NUMBER:

ISSUE NUMBER:

ISSUE DATE:

PURPOSE

To define the responsibility for requesting and administering company certifications, data requests and data handling for Unclassified Technical Data (UTD) disclosing Military Critical Technology (MCT), obtained as a result of Certification under the U.S.-Canada Joint Certification Program.

GENERAL

In 1985, the United States and Canada signed a Memorandum of Understanding (MOU) that established the U.S.-Canada Joint Certification Program. As stated in the MOU's "Joint Terms of Reference for the Joint Certification Program", the program was established "to certify contractors of each country for access, on an equally favourable basis, to unclassified technical data disclosing critical technology". This information is controlled in the U.S. by DoD Directive 5230.25 and, in Canada, by the Technical Data Control Regulations (TDCR). Under each Nations' laws, the U.S. Department of Defense and Canada's Department of National Defence may withhold such technical data from public disclosure.

To meet the provisions of the U.S. Department of Defense Directive 5230.25 and the Canadian Department of National Defence Technical Data Control Regulations, so that (***company name***) may have access to certain sensitive information necessary for our business operations, the procedures outlined in this document must be followed.

Use and disclosure of unclassified technical data obtained by (***company name***) under these procedures must be restricted to the purpose identified to the government agency when the data release was requested. If additional uses are identified after receipt of the data, prior approval must be obtained from the appropriate government agency by (***company name***) using the Supplementary Data Request procedures identified in this document.

*** NOTE ***

Employees are advised that illicit use or disclosure of this data, especially unauthorized export, may result in criminal prosecution of the individual(s) responsible, including officers of the company. As well, serious penalties for the company may result, such as revocation of certifications and exclusion from the export process.

PROCEDURES

1.0 Certification Procedures

Certification, as required, shall be sought for each of (***company name***) "scope of activities", i.e., current and planned products and services, which fall within the definition of military critical technology. Each physically separate facility or division shall apply separately for certification.

Certification submission requests shall be completed by the Custodian (***Technical Data Librarian/Facility Security Officer/Project Administrator***) using form DD 2345 Military Critical Technical Data Agreement, and shall be signed by the (***Vice-President Contracts and Pricing/Delegated Company Official***) prior to submittal to the U.S.-Canada Joint Certification Office in Battle Creek, Michigan.

Additional certifications may be required to permit (***company name***) to obtain unclassified technical data for a proposal or a contract. As soon as such a need becomes apparent, the Custodian should be advised of the new "scope of activity" requirement so that the Custodian can determine if an amendment to the existing certification is required in the area identified as "Description Of Relevant Business Activity" on the form DD 2345.

The Custodian shall be responsible for administering and maintaining a record of both submitted and approved certifications and their respective scopes of activity. The Custodian shall also be responsible for requesting renewal of those certifications that are required at the end of the five year period.

2.0 Data Request Procedures

As the need arises for (***company name***) to obtain unclassified technical data for a proposal or contract, the Custodian shall be advised of the data required and the purpose(s) for which the data will be used.

The Custodian shall complete the appropriate Data Request and submit it to the government agency which owns or controls the data required. As a minimum, the Data Request should include the following:

- A copy of the companies DD 2345;
- Detailed information on the data required;
- A statement of the intended data use.

The request should be made on company letterhead.

The Custodian shall be responsible for maintaining a record of both submitted and approved requests for unclassified technical data.

Data Requests are reviewed by the government agency which owns or controls the unclassified technical data. Release approvals may be accompanied by additional controls or measures specified by the government agency to safeguard the data. Such additional controls or measures shall be implemented by (***company name***), and may be subject to audit by the government agency which demanded them, or, by the government Industrial Security Program officials.

3.0 Supplementary Data Requests

Should additional business uses be discovered for specific unclassified technical data, after release to (***company name***), employees shall advise the Custodian so that a Supplementary Data Request can be submitted to the government agency which owns or controls the data. Employees shall not use the unclassified technical data for any other purpose other than that for which the data were released to (***company name***).

4.0 Data Release Procedures

The Custodian shall receive the unclassified technical data when it is released by the government agency. Receipt shall be recorded and restrictive markings shall be checked and recorded by the Custodian prior to release of the data to the division of project which has the primary need for the data.

If the unclassified technical data has not been marked as such by the government agency prior to release to (***company name***), the Custodian shall mark the data appropriately on receipt.

The Custodian shall release the data to the appropriate division's or project's data handling facility (e.g., Engineering Data Records, Program Data Bank, System Administrator). Any additional controls or restrictions imposed by the releasing agency shall be highlighted by the Custodian to the division or project receiving the data.

WARNING

Technical Data received through the Joint Certification Program cannot be released to any employee of the company who is not a Canadian or U.S. Citizen or an officially designated Permanent Resident of Canada or an Intending Citizen of the United States.

5.0 **Data Handling Responsibility**

The receiving division or project is responsible for implementation and maintenance of the controls and measures appropriate to safeguarding the specific data, as well as any additional controls and measures imposed by the releasing agency.

Each employee who uses the unclassified technical data, received through this program, is responsible for its care while in its immediate charge, and for its safe return when use is finished.

6.0 Use and Disclosure of Unclassified Technical Data

Employees shall use unclassified technical data only for the purpose for which it was released to (***company name***). Such purpose is recorded on the Data Request. If additional uses for the data are identified after receipt by (***company name***), a Supplementary Data Request must be made and agency approval granted prior to any such additional use of the data.

Unclassified technical data shall be disclosed by (***company name***) only for the purpose specified in the Data Request. Such disclosures would include, for example, proposals or contractually -deliverable data. No disclosure of unclassified technical data is permitted other than for the reasons identified to the government agency in the Data Request.

Casual requests for unclassified technical data from companies or individuals shall be denied. (***Company name***) may direct such companies or individuals to the government agency which owns or controls the data and/or to the U.S.-Canada Joint Certification Office.

WARNING

Violators of Export Control Laws are subject to criminal prosecution.

7.0 Disposal of Unclassified Technical Data

Disposal of unclassified technical data is the responsibility of the division or project that had primary need for the data.

Disposal methods may include, for example, return to the government agency or shredding by (***company name***). Disposal conditions will vary depending on its sensitivity. Employees should contact the Custodian for guidance regarding disposal requirements for the specific data involved.