Incoming Export Controlled Information/Item Questionnaire

1. What type of information/material is being disclosed to you or is coming to UVU?

(Check all that apply)

☐ Technical Data ☐ Software ☐ General Information

☐ Hardware ☐ Equipment ☐ Other:_____

2. How will information/material be marked to clearly distinguish it as Export Controlled?

UVU Guidelines: At minimum, information/materials should be marked as "Export Controlled – Restricted Access." However, for all information/materials related to Department of Defense funded research, all technical documents containing export-controlled information should be marked as follows (per DoD Directive 5230.24):

"WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25."

3. List all UVU personnel that will have access to the information/material:

(If needed, additional personnel can be listed at the end of document)

Name: _____ Position:_____

☐ US Citizen ☐ Green Card ☐ Foreign National/Current Citizenship _____

Name: _____ Position:_____

☐ US Citizen ☐ Green Card ☐ Foreign National/Current Citizenship _____

UVU Guidelines: Under current export control regulations, export controlled information **cannot** be shared with foreign nationals at UVU unless an Export License has been obtained specifically for that person to receive the export controlled information. At a minimum, all personnel who are legally allowed access to controlled information/material should be clearly identified.

4. How will the information/material be physically stored and access controlled while at UVU?

UVU Guidelines: At minimum, information or materials should never be left unattended or unprotected. When not in your possession or when unattended it must be stored in a locked location (e.g., file cabinet or drawer) and if possible stored in a single location. Try to minimize the number of copies made. Electronic information should be maintained as password protected and/or encrypted files and whenever possible stored on local hard-drive and not on shared or networked drives/servers. Foreign national visitors (e.g., visiting scientists or tour groups) should always be escorted when they are in areas where restricted information, equipment or activities are present.

5. Will you be generating any work product(s) as a result of this activity (e.g., technical data, equipment/hardware, software, materials, reports or other information)? ☐ Yes ☐ No

If yes, please describe what will be generated and how it will be used:

6. Will graduate students be performing thesis work with information/material? ☐ Yes ☐ No

(If yes, please list students. Additional students can be listed at the end of document):

Name: _____ Position:_____

☐ US Citizen ☐ Green Card ☐ Foreign National/Current Citizenship _____

7. If required, how will work products (e.g., reports) or technical data be shared or returned?

UVU Guidelines: In general, controlled information can be sent as hard copy or CD/DVD via FedEX or registered mail (signature required) or emailed as password protected or encrypted files.

8. When the work is completed, how will information/material be returned or disposed?

UVU Guidelines: In general, when you are finished with export controlled information it should be returned or destroyed pursuant to the terms and conditions under which it was obtained.

When destroying export-controlled information/materials:

- All physical items (hard copies or items) should be shredded, torn or dismantled such that the controlled technology or information is rendered indistinguishable and cannot be reconstructed.
- All electronic files should be deleted using approved software or other sponsor approved measure.