Universities have certain obligations when they sign a software license that includes a requirement that the university comply with export regulations. Software is made available to students, staff, faculty and visitors, including foreigners, in open computer labs, specialized department computer labs, in classes and as part of research they may be performing.

**Non-encryption Software**

**A. EAR**

Under the Export Administration Regulations (EAR), software or technology is exported to foreign nationals if they can visually inspect equipment and facilities, engage in oral exchanges of information either in the United States or abroad, or they travel abroad and apply personal knowledge or technical experience they gained at a U.S. university. 15 CFR § 734.2(b)(3).

However, there are various exemptions from the applicability of the EAR. These include: publicly available software (except encryption software on the Commerce Control List) that is already published or will be published, software that arises during or as a result of fundamental research, software that is educational, and software that is included in certain patent applications. 15 CFR §734.3(b). Software is already published or will be published if it is available for general distribution for free or for a cost that does not exceed the cost of reproduction and distribution. 15 CFR §734.7(b). This would cover all commercially available software. Educational software is that which is released by instruction in catalog courses and associated teaching laboratories at universities. 15 CFR §734.9. This would cover specialized software that is not generally published but is used as part of university classes or is available in department computer labs. If the software or technology is developed as part of fundamental research it is also exempt from the EAR. Fundamental research is basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community.

**B. ITAR**

If the software or technology is regulated under the International Traffic in Arms (ITAR) regulations, different considerations apply. Export is defined under ITAR to include oral or visual disclosure to or the transfer of technical data to a foreign person, either inside or outside the United States. 22 CFR §120.17(4). Technical data includes software, defined in 22 CFR §121.8(f), that is directly related to defense articles. 22 CFR §120.10(4). Software is defined as including “system functional design, logical flow, algorithms, application programs, operating system and support software for design, implementation, test, operation, diagnosis and repair” that is directly related to defense articles. 22 CFR §121.8(f). If a university has software or technology that is regulated under ITAR it is not possible to get a license to permit foreigners to see the software. 22 CFR §120.1(c). In this case those persons would have to be screened from access to this software.
Under ITAR, software is not covered if it is “commonly taught” in universities, is in the public domain or is part of basic marketing information on the function or purpose or general system descriptions of defense articles. Information is in the public domain if it is published and generally accessible to the public:

1. Through sales at newsstands and bookstores;
2. Through subscriptions available without restriction;
3. Through second class mailing privileges;
4. At libraries open to the public;
5. Through patents;
6. Through unlimited distribution at conferences, meetings, seminars, trade shows or exhibits generally accessible to the public in the U.S.;
7. Through public release (unlimited distribution) in any form after approval by the cognizant government agency;
8. Through fundamental research in science and engineering at accredited universities in the U.S. if the resulting information is ordinarily published and shared broadly in the scientific community.

22 CFR §121.11(a)

Thus, there should not be a problem with foreign students’ access to software available in most places on campus.

Encryption Software

A. EAR

The definition of export for encryption software is different than the definition of export of other items subject to the EAR. Export of encryption source code and object code is defined as actual transfer out of the United States, transfer in the United States to an embassy or affiliate of a foreign country or:

downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo optical, photoelectric or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code.

15 CFR §734.2(b)(9).
If the software constitutes encryption source code and object code on the Commerce Control List and in electronic form or media (computer diskettes or CD-ROMs), the university will need a license from the Department of Commerce to export it to any country except Canada. If the encryption software is controlled under ECCN 5D002 for encryption item (EI) purposes, even if it is already published or part of fundamental research, a university would have to have a license to export it.

In addition, a university cannot provide technical assistance, including training and consulting, to foreign persons with the intent to aid them in developing or manufacturing outside the United States encryption software that, if it was of U.S. origin would require a license because it is controlled under ECCN 5A002\(^1\) or 5D002\(^2\) of the Commerce Control List. Technical assistance may be exported to nationals of the countries listed in Supplement 3 to part 740 of the EAR\(^3\) (except for technical assistance to government end-users for cryptanalytic items), and only if the university submits an encryption review request to the Bureau of Industry and Security in the Commerce Department (BIS) by the time of export.

However, if the encryption software and accompanying object code is publicly available, not controlled for EI reasons under ECCN 5D002 and is not mass market encryption software with a symmetric key length greater than 64-bits controlled under ECCN 5D992, it can be exported without an export license or exception if: 1) it is published, 2) it arises during or results from fundamental research, or 3) it is educational (released as part of instruction in catalog classes and labs). However, the BIS has to be notified.

In addition, no license or exception is required for encryption items under ECCNs 5A002 and 5D002 if they meet all of the following criteria:

a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
   1. Over-the-counter transactions;
   2. Mail order transactions;
   3. Electronic transactions;
   4. Telephone call transactions.

b. The cryptographic functionality cannot be easily changed by the users;

c. Designed for installation by the user without further substantial support by the supplier;

\(^1\) Systems, equipment, application specific “electronic assemblies”, modules and integrated circuits for “information security”, and other specially designed components therefor. NOTE: Phrases in quotes are defined in 15 CFR Part 772.

\(^2\) Information security software.

\(^3\) Austria, Australia, Belgium, Cyprus, Czech Republic, Estonia, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom.
d. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter’s country in order to ascertain compliance with the conditions described in paragraphs (a) through (c).

However no items classified under ECCNs 5A002, 5D002, 5E001 5A992, 5D992 and 5E992, including mass market software, can be exported to Cuba, Iran, North Korea, Libya, Sudan or Syria.

Despite this restriction, teaching or discussion in the academic setting of information regarding cryptography in general, even if foreigners are present, is permissible. Printed material such as textbooks that sets out encryption source code is not subject to the EAR, but if the encryption source code is in electronic form or media those forms of the source code are subject to the EAR.

B. ITAR

If the encryption software is controlled under ITAR, there are various exemptions and exceptions available for export of technical data and classified defense articles. However, these exemptions do not apply to exports to proscribed destinations.⁴

⁴ Belarus, Cuba, Iran, Libya, North Korea, Syria, Vietnam, Burma, China, Haiti, Liberia, Somalia, and Sudan. 22 CFR §126.1(a). In addition, any country subject to a United Nations Security Council resolution is also a prohibited destination.