## DTCC Free Open Source Software Use

You may ONLY use approved DTCC Free Open Source Software (FOSS) in DTCC applications built and run on DTCC servers.

You may not use DTCC approved FOSS to develop an application that will run at the customer/client site(s). This restriction includes any plug-in, applet etc. that is DTCC code running in a client’s browser and/or machine. Should you require this capability, you MUST meet with Architecture Office and Technology Risk Management to review your request. Please be advised that Senior Management Approval will be required.

## About DTCC Approved FOSS

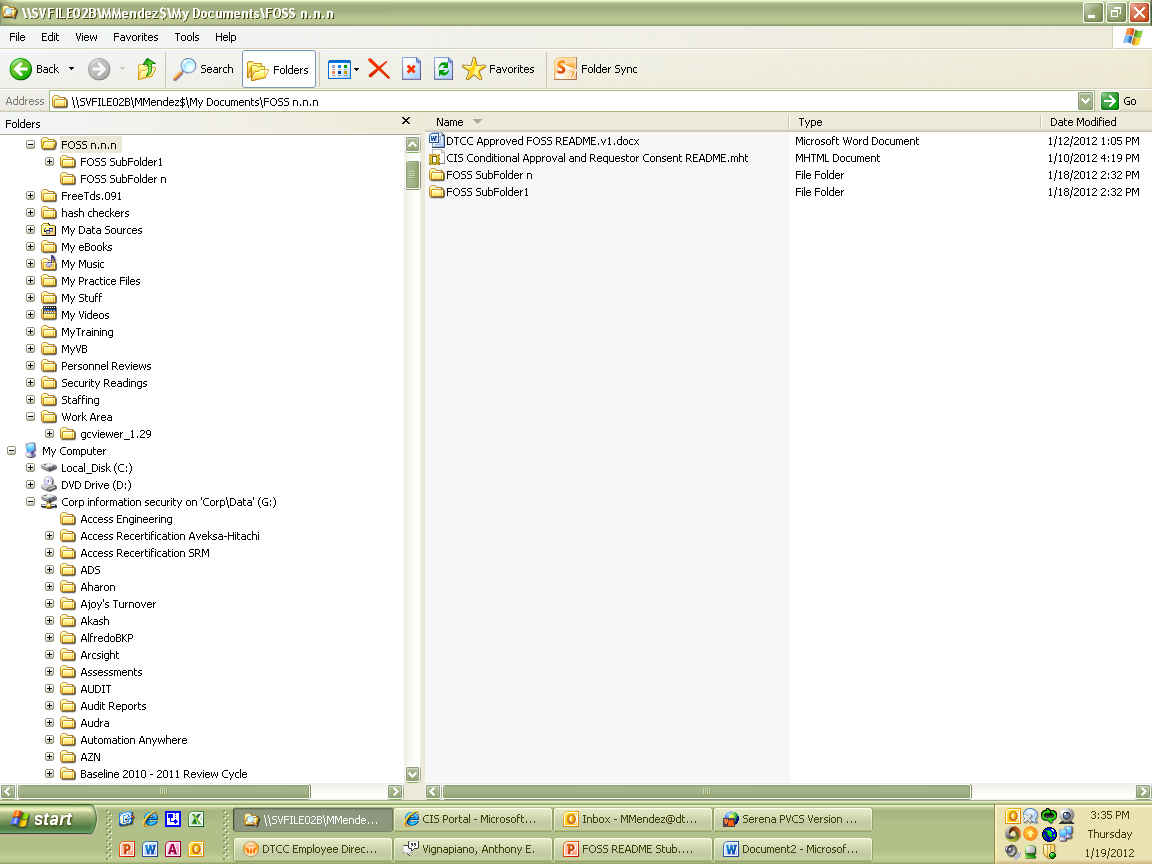
All approved FOSS will be migrated by TRM to either SCM\_COMMON\_RUNTIME via SCM request system or placed in the Share Point site as the starting point for non PVCS managed FOSS distribution.

Approved FOSS will fall into one of three categories:

1. Software Library – migration will go to PVCS and becomes available to all users in **SCM\_COMMON\_RUNTIME/FOSS**. This will be FOSS you will include in your PVCS application project. The FOSS is identified by its name, version, and PVCS version label.
2. Desk Top – migration will go to Share point so that it may be distributed in the present manner by IC**.** For further information, please contact Architecture Office.
3. Server Software – migration will go to Share point so that it may be distributed in the present manner by IC**.** For further information, please contact Architecture Office.

FOSS is organized in a dependent folder tree structure. The versioned FOSS dependency chain is made by the FOSS creator. Technology Risk Management downloads that tree structure and implements it as is. Using the illustration below:

**FOSS n.n.n** is the top level folder identifying the approved FOSS version.



FOSS SubFolder1 . . . FOSS SubFolder n

- Illustrates FOSS creator structure as downloaded from Internet. See FOSS creator readme files to determine dependencies and options

Approved FOSS folder structure and content (source or jar/exe/other) placed in FOSS n.n.n folder

1. Subordinate to main FOSS level may be a sub-tree folder(s). This will occur when the main FOSS has dependent/dependencies or choices as created by the FOSS creator – see text in **red** above
2. DTCC Approved FOSS README.docx and any DTCC guidance and/or use constraints regarding this FOSS version. Every user of this FOSS is required to adhere to these documents.
3. Approved jar/source/exe/etc. (Depending on what was requested and type of FOSS), any README, samples, guidance etc. that was available at the time the FOSS was downloaded from the Internet – see text in **green** above

## Approved FOSS Information You Need to Be Aware – Vulnerabilities, Dependencies, FOSS Packaging

Click this link to access this FOSS record:

[Wamp Server 2.2 FOSS Record](https://saarap01/archer/default.aspx?requestUrl=..%2fcontent%2fview.aspx%3fPageID%3di7361%26Id%3d7373809)

This link will take you to Technology Risk Management (TRM – formerly CIS) Portal record. Here you will find important information about the FOSS analysis that you should be aware of.

Key record sections are:

### General Information Section

* Contains the indicative information about the FOSS request; FOSS name and version, FOSS URL, request date, requestor, FOSS type (desk top, server, software library), etc.

### Security Review Section

Approved FOSS does not mean it is free of vulnerabilities. This section provides you with the analysis performed by TRM team.

* Vulnerability Information and links to web sites to assist you in understanding vulnerabilities found at the time the FOSS review was undertaken.
* Fortify Report (if available) created at the time of FOSS review to assist you further in understanding vulnerabilities. If present, it is intended to help you in assisting you in your project planning.

### “This artifact depends on . . .” Section

* If the FOSS record has dependencies on other FOSS record(s), this section will contain as many hyperlinked rows as the FOSS item depends on.
* Clicking on the “Tracking ID”, will take you to that dependent record. You can review each dependent record’s “Security Review” section to view the FOSS review findings.
* If that record has further dependencies, “This artifact depends on . . .” section will contain hyperlinks which you can select and view those records.

### “This artifact is used by . . .” Section

* If the FOSS record you are viewing is used by another FOSS, the user of this FOSS record will be displayed.
* Clicking on the “Tracking ID”, will take you to that record.
* This information may be useful to you so that you understand the record you are accessing may be both a record that uses other FOSS and may be used by other FOSS.

### License Information Section

* Contains every license the governing the FOSS record you are viewing.
* A license record(s) will always be displayed for each FOSS record and dependent record.

### FOSS Admin Section

* Contains requestor request and may contain additional information the requestor may need to know when using the FOSS. Such information may be compile and/or other software requirements. This section may contain link(s) to Internet to provide additional reference material the FOSS user may need to know,

## Contact Technology Risk Management

FOSS is a constantly evolving and changing landscape. TRM FOSS team makes every attempt to provide you with the information you need to have. However, some of that is based on interpreting and translating the FOSS creator’s guidance, and evaluating available vulnerability information as of a point in time.

What is published today may be out of date tomorrow. If you know of updated or alternate information, please share that with TRM. TRM will evaluate it and update the records for everyone’s benefit.

Please send an email to “SILC SEC DOC” with the subject line “Request FOSS Assistance”, enter your question(s) and/or update information in the message body. A Technology Risk Management team member will contact you.