PennState
Institute
for CyberScience

ICS-ACI Policy Series

ICS-ACI-P040 Software Acceptable Use Policy

This is part of a series of documents that make up the formal policies adopted by the Institute for CyberScience at the Pennsylvania State University.

Last Updated: June 30, 2016

Contents

Overview

This policy defines the policy and guidelines for utilization of software and licenses, software installation and maintenance, as well as how additional software can be requested and installed for the Institute of CyberScience - Advanced Cyberinfrastructure (ICS-ACI).

Purpose and Scope

This policy details the management of and acceptable use for ICS-ACI software and licenses, requesting additional software installation and user installation of software. This policy is implemented to ensure fair and equitable access to software and licenses for all ICS-ACI users; it is not intended to inhibit access to software and licenses. All software resources are to be used for research or teaching purposes which are sanctioned by the University. Anyone violating this policy or the policies referenced below is subject to suspension or termination of their user account.

This policy may be extended or modified as needed. All revised policies will be published online.

Waivers and Exceptions

Waivers and exceptions to this policy should be coordinated through the ICS Coordinating Committee and ACI Working Group. Waivers and exceptions may include, but are not limited to, the following:

- Software Stack Modification Timeline
- Additional software support or resources needed that are not captured in the Service Level Agreement (SLA)

These exceptions will be considered by the ICS-ACI staff in conjunction with ICS Coordinating Committee as they are received.

Software Stack Definitions

The ICS-ACI architecture is organized into Service Layers into which software may be installed. The software installed on this system fits into one of three categories addressed by this policy; 1) ICS-ACI Maintained Infrastructure stack, 2) ICS-ACI Maintained Application Stack, and 3) User Software Stack. The ICS-ACI Maintained Infrastructure and Application Stacks are installed and managed by ICS-ACI system administrators (system maintainers). Software on the User Software Stack is introduced and maintained by the system users such as the Principle Investigators (PI) and researchers.

The ICS-ACI Maintained Infrastructure Stack includes software installed at the system level required for the system to exist. This includes operating systems, resource scheduler (e.g. MOAB) and system monitoring and logging software. The ICS-ACI Maintained Application Stack consists of application driving software, such as compilers, communication libraries and data movement software, and widely used application software, such as Python, R or COMSOL. The ICS-ACI Maintained Software Stacks will consist of widely used versions of the software.

The User Software Stack includes software introduced and maintained by investigators and researchers (users) into their own storage space ($HOME, $WORK or $SCRATCH) or into a shared group directory. Investigator (User) software is installed on the software layer. The User Software Stack allows users to keep software that is specialized either in content or in version for their own use. This specialized software can be software that is not widely used around campus and is not installed and maintained for all users by the system administrators. Additionally, both newer and older versions of the system maintained software can be installed and maintained by users as their research requires. The table below lists the high-level software that is included in the software stacks. Please note that this table is not an all-inclusive list of software.

Summary of Software Stacks

ICS-ACI Maintained Infrastructure Stack	ICS-ACI Maintained Application Stack	User Software Stack
Operating System (RH, Windows, ESXi, etc.)	Communication Libraries (MPI, OpenMP)	Legacy versions of software (No longer supported at the system level)
Security Monitoring and Logging (OSSEC)	Compilers	Bleeding edge versions of software (Not yet widely accepted/used or supported at the system level.)
Batch Job Scheduler (MOAB, Torque)	Commonly used Software Applications (e.g. MATLAB, COMSOL, R, Python etc.)	Specialized software (used by small numbers of users)
Configuration Management (Puppet, Atlassian)	File Transfer (Globus)	Specialized modules/libraries for use within ACI maintained software
Nessus		
Satellite Server		

System Software Stack Request Timeline and System Installation Guidelines

ICS-ACI System Maintained System and Application Software Stacks, or the baseline software, will be updated twice a year in baseline deliveries. Each of these baseline deliveries requires a system outage for which users are notified in advance. New software or updates to existing software will be installed during these baseline deliveries. Change requests to the ICS-ACI Maintained Infrastructure and Application Stacks should be made no less than 6 weeks prior to the baseline delivery. The six-week window allows the system maintainers to build a sandbox version of the new environment to run test cases for the various software to ensure smooth transitions. All ICS-ACI users will be sent a reminder to provide requests for new software to be included in the ICS-ACI baseline delivery at least two weeks in advance of the deadline. Software requests made within 6 weeks of the system baseline delivery may be denied, however, they will be considered for the following baseline deliver. The system maintained software may be updated outside of this biannual cycle if security vulnerabilities require immediate action.

User Software Stack Guidelines

User software introduced into the User Software stack, software within a user's storage space, shall be introduced and maintained by the user or group who introduced the software. Users may put software in their directories at any time provided that the applicable responsibilities and requirements for software use are met as documented in this policy. The ICS-ACI system maintainers are not responsible for any software introduced by the user, unless an existing SLA dictates otherwise. Users are responsible for the maintenance and upgrade of the software introduced as well as ensuring that software is free of software vulnerabilities. Furthermore, the user or group introducing the software is responsible for tracking and managing any license or use agreements required for software use.

Users are responsible for maintaining and managing their software for the entire lifecycle of the software (i.e. implementation through removal). Furthermore, the ICS-ACI system maintainers are not responsible for adverse effects (i.e. version compatibility issues) on user software that arises from modifications made to the ICS-ACI Maintained Software Stack.

Please refer to the Responsibilities and Requirements for Software Use sections below for additional guidance.

ICS-ACI Maintained Software Stack Installation Guidelines

ICS-ACI system maintainers are responsible for installing and managing software in the ICS-ACI Maintained Infrastructure and Application Stacks. Software modifications, additions, and removals from the ICS-ACI Maintained Stacks will be completed during the planned baseline deliveries.

Responsibilities

Summary of Responsibilities

Action	ICS-ACI Maintained Software Stack	User Software Stack
Evaluate Impacts of new baseline	ICS-ACI	Researcher
Procurement	ICS-ACI	Researcher
Verify License / Usage agreements for Software	ICS-ACI	Researcher
Track and Maintain Software list on website	ICS-ACI	NA
Alert users of Software changes	ICS-ACI	NA
Scan Software for vulnerabilities	ICS-ACI	NA
Remove Software that presents security vulnerabilities	ICS-ACI	ICS-ACI
Communicate Baseline Delivery Schedule	ICS-ACI	NA

Researcher Responsibilities

Any software that is put into users' group or personal directories as a part of the User Software Stack must meet the following criteria:

1. The software license and usage agreements must be followed
2. Users will ensure that no vulnerabilities and viruses exist to the extent practical (e.g., Malware).
    a. Any software that presents a security risk for the system may be removed from the User Software Stack by system administrators ;
    b. Upon said removal the user shall be notified of the removal including an explanation of the reasons why the software was removed;
    c. Repeated or flagrant offenses will also result in the suspension or termination of user accounts;
3. Additional software introduced by users shall be maintained by the users unless otherwise specified in the ICS-ACI SLA.

Researcher needed software to be installed in the ICS-ACI Maintained Infrastructure and Application Stacks must meet the following criteria:

1. User requests for software modifications on in the ACI Maintained Infrastructure and Application Stacks must be submitted to the i-ASK service center (https://iask.aci.ICS-ACI.psu.edu):
    a. Software requests should be made within the timeframe described above in the Software Request Timeframe section;
    b. The request type should be identified as "Software" on the ticket request;
2. The software, or version of software, must have required capabilities that software currently on the system maintained stacks do not provide
    a. Newer versions of software will only be installed when additional or improved capabilities are made;
    b. The software must have application to and/or be in use by a large number of users;
    c. The software must not introduce an undue maintenance burden, and must be in a mature, stable portion of its lifecycle.

ICS-ACI System Maintainer Responsibilities

ICS-ACI system maintainers (e.g. administrators, operations engineers, system engineers, etc.) are responsible for installing and maintaining the ICS-ACI Maintained Infrastructure and Application Stacks provided with the baseline deliveries. Responsibilities include:

1. To evaluate software for vulnerabilities prior to its installation on the ICS-ACI Maintained Infrastructure and Application Stacks;
2. To deploy and maintain the ICS-ACI Maintained Infrastructure and Application Stacks as part of the ACI system:
    a. Install and maintain software on the ICS-ACI Maintained Infrastructure and Application Stacks;
    b. Upon release of a new version, ICS-ACI will install the new version on its developmental system. Once verified, it will be deployed on the production systems. At this time, the oldest version will be removed from the production system. ICS-ACI will maintain at least

the current release and one previous version of the software package. Users requiring older versions may have this software transitioned into their local directories (User Software Stack);

c. Perform routine security/vulnerability patching through automated mechanisms;

3. Communicate through email to all users of the system any changes to the ICS-ACI Maintained Infrastructure and Application Software Stacks to include new software packages and updated versions (e.g. Operating System upgrades, etc.), and removals; [Login prompts will be used to provide reminders; however, email will be the main communication route that ICS-ACI uses.]
4. Periodically scan the system for software vulnerabilities;
5. Maintain a list of the ICS-ACI software installed on the ICS-ACI Maintained Infrastructure and Application Stacks on the ICS-ACI website;
6. Provide assistance in moving legacy software (i.e. software that is at least two releases out of date) from the ACI Maintained Stacks to the User Software Stack:
    a. ICS-ACI system maintainers will provide assistance in the transition of the software to the User Software Stack. Once the transition has been completed the user assumes all responsibilities for that software (i.e. licensing, use compliance, maintenance);
7. ICS-ACI reserves the right to remove any software application and/or library for the following reasons:
    a. Security Vulnerabilities – Software will be removed immediately without prior warning. After removal is complete the software owner(s) will be notified of the removal with an explanation; ICS-ACI will work with the software owner(s) to evaluate and mitigate the vulnerability; Once the vulnerability has been addressed the software may be re-introduced into the ICS-ACI Maintained Application Stack.
    b. Degradation of system operations – Impacts to system operations will be evaluated to determine what and who have been impacted. In the event it is determined that users are not able to complete their research and/or system availability and integrity have been compromised the software will be isolated immediately. The software requestor will be notified prior to isolating the software;
    c. Violation of License Agreements;
    d. Issues that impact the integrity, availability or confidentiality of the ICS-ACI system functionality.
8. Provide assistance to users needing to compile code:
    a. Requests for assistance must be submitted through the i-Ask Service Center

Requirements for Software Use

To ensure that its software assets derive maximum benefit to the ICS-ACI user community allowing fair and equitable use, and to ensure that ICS-ACI and its users adhere to a standard software policy, ICS-ACI users:

- Shall understand, agree to, and comply with all security policies governing Penn State and ICS-ACI Computer and Network Resources, as well as all federal, state and local laws, including laws applicable to the use of computer facilities, electronically encoded data and computer software;
- Shall use the system to further research objectives and not for personal gain (i.e. prohibits activities such as Bitcoin Mining, etc.);
- Shall not try to exploit and/or probe for vulnerabilities or weaknesses within the system;
- Shall evaluate software to the extent practical for potential and known vulnerabilities prior to introducing software in the User Software Stack;
- Shall assume all responsibility of managing and procuring license(s) as well as ensuring acceptable use for any software residing in the User Software Stack;
- Shall not duplicate copyrighted software not allowed by the software license, except for backup and archival purposes;
- Shall notify ICS-ACI i-ASK Service Center (https://iask.aci.ICS-ACI.psu.edu) of evidence of the use or distribution of unauthorized software. You may not loan or give to anyone any software licensed to ICS-ACI. Under no circumstances may any user use the ICS-ACI licensed software for purposes other than an Educational or Research purposes sanctioned by the University;

Academic License Agreements that reference export controls may require the following notification that all users must comply to applicable U.S. export control laws and regulations. Please see the website for a list of these notifications including:

> "NOTICE: The terms of the Academic License to this software specifically prohibit the use of software (reference https://ics.psu.edu) in conjunction with the design, development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological, or nuclear weapons or nuclear explosive devices, or the development, production, maintenance or storage of missiles capable of delivering such weapons, or for any prohibited military end-uses. In addition, the Academic License terms require that all users be notified that use of this software is subject to applicable U.S. export control laws and regulations and that users must comply with such laws in their use of this software. This notification can be accomplished either in print or via an on-screen display on this notification. Questions about these license requirements and/or export compliance at Penn State in general may be directed to the University Export Compliance Office at Export@psu.edu."

Reference

This policy applies to any person who utilizes resources that are provided and managed by ICS-ACI. In the absence of specific ICS-ACI policies, Pennsylvania State University policies apply. This policy augments the following Pennsylvania State University and ICS-ACI policies:

University Policies

- AD11 – University Policy on Confidentiality of Student Records;
- AD20 – Computer and Network Security;
- AD23 – Use of Institutional Data;
- AD71 – Data Categorization;
- ADG01 – Glossary of Computerized Data and System Terminology;
- ADG02 – Computer Facility Security;
- HR102 – Separation and Transfer Protocol;
- RA40 – Compliance with Federal Export Regulations for Sponsored Research Efforts

ICS-ACI Policies

- ICS-ACI P020 – User Account Policy;
- ICS-ACI P030 – Data Retention Policy;
- ICS-ACI P060 – ICS-ACI SLA Terms and Conditions policy

Visit the Institute for CyberScience on the web at https://ics.psu.edu**.**

This publication is available in alternative media on request.

The Pennsylvania State University is committed to the policy that all persons shall have equal access to programs, facilities, admission, and employment without regard to personal characteristics not related to ability, performance, or qualifications as determined by University policy or by state or federal authorities. It is the policy of the University to maintain an academic and work environment free of discrimination, including harassment. The Pennsylvania State University prohibits discrimination and harassment against any person because of age, ancestry, color, disability or handicap, national origin, race, religious creed, sex, sexual orientation, gender identity, or veteran status and retaliation due to the reporting of discrimination or harassment. Discrimination, harassment, or retaliation against faculty, staff, or students will not be tolerated at The Pennsylvania State University. Direct all inquiries regarding the nondiscrimination policy to the Affirmative Action Director, The Pennsylvania State University, 328 Boucke Building, University Park, PA 16802-5901; Tel 814-863-0471/TTY.