PennState
Institute for Computational
and Data Sciences

ICDS-ACI Policy Series

ICDS-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 Computational and Data Sciences at the Pennsylvania State University.

Last Updated: November 13, 2019

Version History:

Date	Version	Name	Description
	1.0		Initial Release
1/26/17	1.1	Avery Urusow	Formatted Document with ICS theme.
11/13/19	1.2	C. Mann	Formatted Document with ICDS theme.

Contents

1.0 Overview

This document 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 Computational and Data Sciences - Advanced Cyber Infrastructure (ICDS-ACI).

2.0 Purpose and Scope

This policy details the management and acceptable use of ICDS-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 ICDS-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.

3.0 Waivers and Exceptions

Waivers and exceptions to this policy should be coordinated through the ICDS 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 ICDS-ACI staff in conjunction with the ICDS Coordinating Committee as they are received.

4.0 Software Stack Definitions

The ICDS-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) ICDS-ACI-Maintained Infrastructure stack, 2) ICDS-ACI-Maintained Application Stack, and 3) User Software Stack. The ICDS-ACI-Maintained Infrastructure and Application Stacks are installed and managed by ICDS-ACI system administrators (system maintainers). Software on the User Software Stack is introduced and maintained by system users, such as the Principal Investigators (PIs) and researchers.

The ICDS-ACI-Maintained Infrastructure Stack includes software installed at the system level required for the system to exist. This includes operating systems, resource schedulers (e.g. MOAB), and system monitoring and logging software. The ICDS-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 ICDS-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		
ICDS-ACI-Maintained Infrastructure Stack	ICDS-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		

5.0 System Software Stack Request Timeline and System Installation Guidelines

ICDS-ACI-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, of which users are notified in advance. New software or updates to existing software will be installed during these baseline deliveries. Change requests to the ICDS-ACI-Maintained Infrastructure and Application Stacks should be made no less than six 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 ICDS-ACI users will be sent a reminder to provide requests for new software to be included in the ICDS-ACI baseline delivery at least two weeks in advance of the deadline. Software requests made within six weeks of the system baseline delivery may be denied. However, they will be considered for the following baseline delivery. The system-maintained software may be updated outside of this biannual cycle if security vulnerabilities require immediate action.

5.1 User Software Stack Guidelines

User software introduced into the User Software Stack, i.e., 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 ICDS-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 for ensuring that software is free of software vulnerabilities. Furthermore, the user or group introducing the software is responsible for tracking and managing any licenses 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 ICDS-ACI system maintainers are not responsible for adverse effects (i.e., version compatibility issues) on user software that arises from modifications made to the ICDS-ACI-Maintained Software Stack.

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

5.2 ICDS-ACI-Maintained Software Stack Installation Guidelines

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

6.0 Responsibilities

Summary of Responsibilities		
Action	ICDS-ACI-Maintained Software Stack	User Software Stack
Evaluate impacts of new baseline	ICDS-ACI	Researcher
Procurement	ICDS-ACI	Researcher
Verify license/usage agreements for software	ICDS-ACI	Researcher
Track and maintain software list on website	ICDS-ACI	N/A
Alert users of software changes	ICDS-ACI	N/A
Scan software for vulnerabilities	ICDS-ACI	N/A
Remove software that presents security vulnerabilities	ICDS-ACI	ICDS-ACI
Communicate baseline delivery schedule	ICDS-ACI	N/A

6.1 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 and provided with an explanation of 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 ICDS-ACI SLA.

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

1. User requests for software modifications in the ICDS-ACI-Maintained Infrastructure and Application Stacks must be submitted to the i-ASK Service Center (https://iask.aci.ICDS-ACI.psu.edu).

    d. Software requests should be made within the timeframe described above in the Software Request Timeframe section.
    e. 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.

6.2 ICDS-ACI System Maintainer Responsibilities

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

1. Evaluating software for vulnerabilities prior to its installation on the ICDS-ACI-Maintained Infrastructure and Application Stacks.
2. Deploying and maintaining the ICDS-ACI-Maintained Infrastructure and Application Stacks as part of the ACI system, including:

    a. Installing and maintaining software on the ICDS-ACI-Maintained Infrastructure and Application Stacks.
    b. Upon release of a new version, installing 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 systems. ICDS-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. Performing routine security/vulnerability patching through automated mechanisms.

3. Communicating through email to all users of the system any changes to the ICDS-ACI-Maintained Infrastructure and Application Software Stacks, including new software

packages, 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 ICDS-ACI uses.

4. Periodically scanning the system for software vulnerabilities.
5. Maintaining a list of the ICDS-ACI software installed on the ICDS-ACI-Maintained Infrastructure and Application Stacks on the ICDS website.
6. Providing 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. ICDS-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. Removing software applications and/or libraries, if necessary. ICDS-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. ICDS-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 ICDS-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 ICDS-ACI system functionality.
8. Providing assistance to users needing to compile code.
   a. Requests for assistance must be submitted through the i-Ask Service Center.

7.0 Requirements for Software Use

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

- Shall understand, agree to, and comply with all security policies governing Penn State and ICDS-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., 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 the ICDS-ACI i-ASK Service Center (https://iask.aci.ICDS-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 ICDS-ACI. Under no circumstances may any user use the ICDS-ACI licensed software for purposes other than 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://ICDS.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 of 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."*

8.0 Reference

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

University Policies

- AD11 – University Policy on Confidentiality of Student Records
- AD95 – Information Assurance and IT Security
- AD96 – Acceptable Use of University Information Resources
- HR102 – Separation and Transfer Protocol
- RA40 – Compliance with Federal Export Regulations for Sponsored Research Efforts

ICDS-ACI Policies

- ICDS-ACI P020 – User Account Policy
- ICDS-ACI P030 – Data Retention Policy
- ICDS-ACI P060 – ICDS-ACI SLA Terms and Conditions Policy

9.0 GLOSSARY

ACI-b	ICDS-ACI sub-system configured to execute jobs submitted to a variety of queues, i.e. batch processing.
ACI-u	ICDS-ACI User-Specific “Development/Test” interactive subsystem where PIs may specify a system configuration for user-specific interactive sessions, including root access and user-defined software stack.
Batch	Executing or processing of a series of programs (jobs) on a system without manual intervention.
Core	Data processing unit within a server. The total cores per server is dependent upon the vendor’s architecture of the server.
Core Allocation	Amount of physical compute resources purchased by or granted to a user through ICDS-ACI plans.
F&A	Facilities and Administration charge, sometimes referred to as “indirect” or “overhead”.
GPFS	General Parallel File System.
Group	A self-defined set of multiple users—for example, students and researchers in a faculty member’s lab. Such rights as access to storage and allocation of resources can be delegated in an organized fashion by the PI.
Group Storage	Dedicated disk space for storing group-related data or research.
Guaranteed Response Time	The maximum time that it takes for a job to start execution after submission to a queue.
Home Directory	A user’s dedicated disk space for storing personal files, directories and programs. Directory that a user is taken to after logging into the system.
ICDS-ACI	Institute for Computational and Data Sciences - Advanced Cyber Infrastructure.
ICDS-ACI-Burst	Queue to allow usage of compute resources in the ACI-b subsystem above a PI’s physical allocation that are needed for a short time period.
ICDS-ACI-Guaranteed	Queue providing access to the ACI-b subsystem within a guaranteed time, provided request is within a PI’s physical allocation.
ICDS-ACI-Open	Queue to provide user access to idle ACI-b resources that can be used during times when supply exceeds demand.
Legacy Systems	Pre-2015 ICDS computing systems, such as the Lion-X clusters.
Login Nodes	Front-end servers used to log in to the ICDS-ACI compute system.

NAS	Network-Attached Storage.
PI	Principal or Primary Investigator. Person, such as faculty, who is authorized to direct all of his or her research ICDS-ACI resources, e.g. access, storage, compute.
Pre-emption	The act of pausing or stopping a job that is currently processing in order to fulfill terms and conditions to other users under service level agreements.
Scratch Directory	Disk space dedicated for temporary storage of data.
Service Level Agreement (SLA)	Agreement between ICDS and Research PI in relation to research ICDS-ACI resources, e.g. access, storage, compute.
Subsystem	A unit or device that is part of a larger system, e.g., ACI-b.
System	The computing engine along with the software, storage, network, and peripheral devices that are necessary to make the computer function, e.g., ICDS-ACI.
User	A person, such as a student or faculty, who has a user account to use the ICDS-ACI resources.
User Account	The means by which a user can access a computer system. ICDS-ACI has four distinct user accounts: PI, Student, Staff, and Sponsored Guests.
Wall Time	A queue parameter that is set to define the maximum allowable execution time for a job once it has started.
Work Directory	User’s dedicated disk space for storing research data.

PennState
Institute for Computational
and Data Sciences

203 Computer Building
The Pennsylvania State University
University Park, Pa 16802

Email: ICDS@psu.edu
Website: https://ICDS.psu.edu