ICS-ACI Policy Series

ICS-ACI-P030 Authentication and Access Control

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: July 9, 2015

1.0 Overview

The purpose of this policy is not to impose restrictions that are contrary to the Pennsylvania State University's established culture of openness, trust and integrity. The Institute for CyberScience (ICS), through Advanced Cyber Infrastructure (ACI), is attempting to provide a balanced allocation of highly available resources which are easy to access and use. Key to this is an understanding by end users as to how their user account is requested, assigned and maintained.

2.0 Purpose

The purpose of this policy is to effectively manage the lifecycle of ICS@PSU accounts created under the current state and configuration of the ICS-ACI as of the date of the approval of this policy. This policy may be extended or modified to support systems and research user community expansion.

By requesting an ICS-ACI user account, users acknowledge that they have read and understood all ICS-ACI and applicable Pennsylvania State University policies and agree to abide by said policies. Users are also asked to acknowledge their use of ICS-ACI resources in resulting publications and reports with the following statement:

This research or portions of this research were conducted with Advanced CyberInfrastructure computational resources provided by The Institute for CyberScience at The Pennsylvania State University (http://ics.psu.edu).

3.0 Scope

This policy details the criteria for creating a user account, using a user account, transferring an existing user account (created under the former RCC) as well as the termination of a user account. This policy is not intended to inhibit access to services and exists to ensure fair and equitable access to infrastructure and services within ICS. However, use of such services is restricted to facilitating research within the University. All computational resources are to be used for research purposes only. Anyone violating this policy is subject to suspension or termination of their user account.

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 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

4.0 Policy

4.1 Account Requests

An account used to access ICS-ACI resources may also be referred to as an ICS@PSU account. User account creation is governed by the following requirements:

New Users

- ICS-ACI User Accounts are available for all University faculty, students, postdocs and staff already having a University access ID. Accounts for students and postdocs require a faculty sponsor.
- ICS-ACI User Accounts are also available to sponsored guests via a Sponsored Access Account.
- New users must first submit a completed account request form, which is available through the ICS web site at https://accounts.aci.ics.psu.edu.
- New users must agree to posted acknowledgements at the time of an account request before processing of the request will begin.
- Account requests will be processed by an account consultant. Additional approvers may be required as necessary depending upon the details provided in the account request.
- Once an account has been created, the account holder and their sponsor will be notified via email that the account has been processed. The account holder will have a limited time to activate their account, change their initial password and complete any additional authentication requirements (e.g., security questions).

Sponsors

- All accounts must be linked to a Pennsylvania State University faculty sponsor hereafter referred to as a Principal Investigator (PI). Therefore, accounts for individuals other than PIs must be sponsored by a PI who will oversee the use of the account.
- PIs can sponsor multiple users, and users can be sponsored by multiple PIs.
- Sponsored accounts will be verified with the PI sponsor.
- Account sponsors are responsible for promptly notifying ICS-ACI, via an email to iask@ics.psu.edu, if they are leaving the University or if any of their sponsored accounts should be terminated.
- PIs may be asked periodically by ICS-ACI to review the accounts that they sponsor.
- PIs will be notified when an account they sponsor has potentially been misused. Additional actions, including the suspension or termination of the sponsored account, may be taken at the discretion of ICS-ACI account managers. Please see the "Enforcement" section later in this policy.

Advanced Users

- Requests for elevated permissions on ACI instances will be kept to a minimum, while still enabling users to accomplish legitimate research needs. All user accounts must operate under "least privilege" mode during normal daily use.
- Users with the capability for elevated permissions are not permitted to enable elevated permissions for other accounts.

Administrators

- All account requests and modifications as well as related communications will be stored based upon the audit record storage requirements of the Institute for CyberScience.

4.2 Account Types

The following account types exist for ICS-ACI users:

Account Type	Description
Principal Investigator (PI)	A Pennsylvania State University faculty sponsor typically leading a research effort. PIs may sponsor any number of accounts, but these accounts must be used for research only. PIs are responsible for all of their sponsored account users. These accounts are subject to periodic review and will have to be renewed if the sponsoring faculty or the account holders change their University affiliation or fail to comply with Penn State or ICS-ACI account policies. All user accounts will be assigned resources and job priority based on the allocations and priorities of their sponsoring PI. User IDs are based on the PI's Penn State access ID.
Students/Postdocs/Researchers	Any graduate student, undergraduate student, postdoc or other researcher supporting a PI's research. User ids are based on Penn State access IDs.
Staff	Any Penn State employee supporting a PI's research. User ids are based on the employee's Penn State access ID.
Sponsored Guests	A person supporting a PI's research who is not already affiliated with Penn State University and who works closely with a PI. User IDs are based on the sponsored guest's Penn State Sponsored Access Account ID.

4.3 Account Attributes

Accounts are configured with the following attributes and associated data storage capacities:

Naming	Penn State employee/student user ID or Sponsored Access Account user ID
Authentication	Central – no user accounts may use system or service-local authentication tokens
Characteristics	Must meet minimum requirements per University policies; password change every 180 days
Systems Access	Dependent upon the PI's ICS-ACI plan and associated SLA
Job Submission	Dependent upon the PI's ICS-ACI plan and associated SLA
Storage Capacities	Home Directory – Default 10 GB (backed up) Work Directory – Default 128 GB (backed up) Group Storage – Default 5 TB (Allocation varies with SLA and is fee-based; backed up)
Scratch Directory	One million files (**NOT** backed up; routinely deleted after 30 days, but potentially earlier under exceptional circumstances)
Wall Time	Default 24 hours for batch jobs; dependent upon the PI's ICS-ACI plan and associated SLA
Software	Access to existing pre-installed packages

Special requests should be submitted via an email to iask@ics.psu.edu and are subject to faculty defined governance.

4.4 Account Modifications

Requests to change key account attributes, including password resets, must be submitted to iask@ics.psu.edu . All account modifications must be approved by an ICS-ACI account consultant and verified by the sponsor of the account.

4.5 Account Lifecycle

The following table lists the possible states for an ICS@PSU account:

Active	Direct login possible
Active/Pending	Login requires additional automated interaction (e.g., password change)
Suspended	Login requires a state change initiated by the ICS-ACI Accounts Maintenance Team
Inactive	Login requires a state change initiated by either the end user or the ICS-ACI Accounts Maintenance Team
Stale	Account has been Inactive for more than one year and is pending additional action
Deleted	Previously existing account is removed from the accounts system; audit trail maintained

The lifecycle of an account is dependent upon the user account type. The following table lists the maximum authorization periods for the different account types:

Faculty/PI	As long as University affiliation is maintained or upon request for change to "Inactive"
Students/Postdocs/Researchers/Staff	Two years or as authorized by the Sponsor; annual review
Sponsored Guests	One year or as authorized by the Sponsor; annual review

Faculty/PIs who leave the University will maintain their ICS@PSU account as long as their original Penn State Access ID remains active. See Identify Service's "Access Account Deactivation and Extension" site for more details including the default duration. The determination as to whether or not a refund will be issued for any unused services that were already paid for will be outlined in the signed Service Level Agreement (SLA) that originally granted access to ICS-ACI services.

Faculty/PIs who leave the University and whose ICS@PSU account has transitioned into at least a "Suspended" state can reacquire an ICS@PSU account by requesting a Sponsored Guest account.

Accounts may be labeled as "Suspended" in certain situations at the discretion of the ICS-ACI Accounts Maintenance Team. Situations where this can occur include:

- Any violation of University or ICS-ACI policies and procedures. ICS-ACI policies and procedures are available at https://ics.psu.edu/advanced-cyberinfrastructure/policies.
- Possible account compromise.
- Not meeting password change requirements.
- Loss of Pennsylvania State University affiliation (in which case the user may be eligible for a sponsored guest account).
- Upon request of a sponsor who oversees the use of the account.
- Termination of the last SLA between the PI and ICS-ACI.

An automated process will identify "Inactive" accounts that have not been accessed for at least one year. These accounts will be labeled as "Stale" and will be included in a monthly report that is reviewed by the Accounts Maintenance Team for potential additional action. Accounts labeled as “Stale” will pass through the following process to determine their next state:

- The account holder and any associated sponsor will be emailed weekly for a one month period. These notifications will inform them that the account has not been used for at least one year and is subject to additional action. The potential additional action will be clarified in the message.
- After one month of weekly notification emails, an attempt will be made to contact the account holder, and any associated sponsor, by phone to inform them of the potential additional action.
- If these communications fail, additional action as determined by the Accounts Maintenance Team will be taken.
- All accounts except for "Deleted" can be restored to “Active” status by submitting a new account request form.
- Accounts that have been deleted and that are re-created under the same user ID will not automatically have access to the same resources with which they were previously bound without additional coordination between the account sponsor and the Accounts Maintenance Team.

4.6 Account Deletion

Deletion of an account does not necessarily mean that the data associated with the account will also be deleted. The handling of any data associated with an account is discussed in the policy ICS-ACI-P020: Data Protection and Retention.

4.7 Account Transfer and End User Status Changes

User accounts are only to be used by the individual to whom the account is assigned. Although data associated with an account may be transferred to another individual via processes outlined in ICS-ACI-P020: Data Protection and Retention, a user account itself may not be transferred to any other individual.

Faculty/PIs who leave the University may transfer their sponsored accounts to other Faculty/PIs upon mutual agreement of all parties involved and in coordination with the ICS@PSU Accounts Maintenance Team. The state of a sponsored account will parallel the state of the associated sponsoring account, with the exception of any sponsored account that previously has had separate actions taken against it.

Account holders are expected to notify ICS-ACI of any status changes via a service desk request so that a determination can be made as to any necessary changes to accounts. This requirement is in addition to the requirements outlined in Penn State Policy HR102: Separation and Transfer Protocol.

4.8 Access Control

All access to ICS-ACI resources should only be executed in a secure manner:

- All account credentials must be stored and transmitted in a manner meeting University and ICS-ACI requirements. As an example, "telnet" is not a permitted communications protocol for accessing ICS-ACI resources since it passes login credentials in unencrypted form.
- Account holders are not permitted to enable "Guest" accounts or anonymous access to data or services hosted on ICS-ACI resources.

- ICS-ACI will provide a list of approved remote access mechanisms both on their web site and in the account approval message to end users.

Always remember: ICS-ACI personnel will **NEVER** ask you for your password.

4.9 Compromise Response

If you suspect that an account compromise may have occurred or if you identify a situation that could potentially lead to an account compromise, then it is your responsibility to report it. The following reporting structure should be followed with progression down the list if you feel that the entity you are reporting to is not responding adequately to the situation:

- Principal Investigator
- ICS-ACI Security
- ICS-ACI Administrative Staff
- Penn State Security Operations and Services

When ICS-ACI is made aware of a potential compromise, any potentially compromised account is labeled as "Suspended" (see the "Account Lifecycle" section earlier in this policy) and any potentially compromised node is removed from network connectivity and seized. If Penn State Security Operations and Services (SOS) is not already aware of the compromise, then a report is submitted to them as well. If the compromise is validated, the node is fully scanned for any Personally Identifiable Information (PII) or other critical data and a report is submitted to SOS. Once mitigation instructions have been provided by SOS, the node is wiped and rebuilt.

5.0 Enforcement

All account policies exist to facilitate research. Any PI, Faculty, Student or Sponsored Guest violating any of the above policies are subject to immediate suspension and/or termination of their account. Data will be retained and can be transferred to the PI. Any employee, student or visitor found to have violated this policy may be subject to disciplinary action by their administrative unit, the College, or the University.

6.0 Supporting Documents

ICS-ACI-P020: Data Protection and Retention

GLOSSARY

ACI-b	ICS-ACI sub-system configured to execute jobs submitted to a variety of queues, i.e. batch processing
ACI-u	ICS-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 ICS-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.
ICS-ACI	Institute for CyberScience - Advanced Cyber Infrastructure
ICS-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
ICS-ACI-Guaranteed	Queue providing access to the ACI-b subsystem within a guaranteed time provided request is within a PI's physical allocation
ICS-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 ICS computing systems, such as the Lion-X clusters
Login Nodes	Front end servers used to login to the ICS-ACI compute system
NAS	Networked Attached Storage
PI	Principal or Primary Investigator. Person, such as faculty, who is authorized to direct all of his or her research ICS-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 ICS and Research PI in relation to research ICS-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. ICS-ACI
User	A person, such as a student or faculty, who has a User Account to use the ICS-ACI resources

GLOSSARY

User Account	The means by which a user can access a computer system. ICS-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

Version History:

Date	Version	Name	Description
	1.0		Initial Release
6/12/15	1.1	Derek Leydig	Minor Corrections and Updates
6/28/15	1.2		Clarification on Faculty/PIs leaving the University.

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

This publication is available in alternative media on request.