



ICS Domain Acceptable Use Policy

I. Purpose

The purpose of this Policy is to ensure the security, privacy, and stability of the Idaho Consolidated Services (“ICS”) Domain system, by detailing the inherent risks and provide a policy of standards and guidance to the Administrators that manage the system and those risks.

II. Description of the ICS Domain

ICS Domain is the central repository of all User accounts and security information for resources that are used and accessed by Idaho State Agencies within the State Network.

The ICS Domain is built upon a single forest, single tree model with a dedicated Forest Root of idaho.gov which contains the Forest Objects and by default the administrative accounts and groups. This root domain is managed by Enterprise Domain Administrators at the OCIO and by Organizational Unit Administrators from participating agencies that manage their own logical Organizational Units hierarchy.

III. Definitions

- A. Active Directory:** Active Directory is Microsoft’s directory service that stores information about objects on a network and makes this information available to users and network administrators. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with a hierarchical view of the network and a single point of administration for all network objects allowing administrators to assign policies, deploy software, and apply critical updates to an organization. Active Directory is designed for distributed networking environments.
- B. Administrative Account:** A login account with elevated privileges for the purpose of system administration.
- C. Administrator:** Any State employee, Contractor employee, vendor, instructor, and temporary affiliates, who has full or limited administrative rights to access to computer accounts on the ICS Domain.
- D. Domain Acceptable Use Policy (“DAUP”):** The policy set forth herein.
- E. Enterprise Administration:** Administration of the top-level Active Directory infrastructure.
- F. Enterprise Domain Administrator:** A systems administrator allowed administrative privileges for the top-level Active Directory infrastructure.

- G. Enterprise Services Oversight Committee (“ES OC”):** A sub-committee of ITRMC created to oversee the development and operation of high quality, reliable statewide enterprise IT services provided by the Department of Administration.
- H. Group Policies:** Group Policy is a set of rules which control the working environment of user accounts and computer accounts. Group policy provides the centralized management and configuration of operating systems, applications and users' settings in an Active Directory environment.
- I. ICS Domain Administration Team:** The OCIO Server Administration team. The ICS Domain Administration Team may also include IT staff from other agencies, subject to the approval of the Enterprise Services Oversight Committee.
- J. Office of the Chief Information Officer (“OCIO”):** A unit of the Department of Administration which serves all State Idaho agencies, commissions, boards, institutions, etc. with information technology support.
- K. Organizational Unit:** A division or unit within a top-level Active Directory Domain used to create and manage objects. Organizational Units are assigned to a State of Idaho agency, commission, board, institution, etc.
- L. Organizational Unit Administrator:** An individual with administrative rights to computer accounts on the ICS Domain in an Organizational Unit.
- M. Service Accounts:** This is the Windows account that the operating system process uses when it hosts a service.
- N. State Network:** The state of Idaho’s internal network infrastructure that connects all state agencies into one data communication TCP/IP network – the state network includes the Capitol Mall Fiber Infrastructure (CMFONI) and agencies connectivity into the Capitol Mall.
- O. User:** a user is a person who uses a computer or Internet service. In order to identify oneself, a user has an account (a user account) and a username.

IV. Requirements of Administrators

- A.** Administrators, as defined above, agree to comply with the conditions outlined in this Policy, as evidenced by each Administrator’s signature.
- B.** Only Administrators that have been granted permission by the Enterprise Services Oversight Committee (ESOC) or its designated representative are authorized access to manage or make changes to the ICS Domain.
- C.** Administrators understand and agree that the ICS Domain is provided to support the State Network; any other uses, including those that jeopardize the integrity of the ICS

Domain, the State Network, or the safety of Users, and/or are otherwise illegal, are strictly prohibited.

- D. By using or accessing the ICS, all Administrators agree to comply with the following:
 - 1. This Policy;
 - 2. Other applicable State policies as established by the Information Technology Resource Management Council (ITRMC);
 - 3. State policies which may be implemented from time to time;
 - 4. Executive Orders issued by the Governor, State of Idaho; and
 - 5. All applicable federal, state, and local laws and regulations.
- E. Administrators understand and agree that the OCIO reserves the right to revoke any Administrator's rights to the ICS domain, as necessary.
- F. Administrators understand and agree that the ICS Domain will evolve over time and, as a result, their respective responsibilities may change or expand.
- G. Administrators agree that they will respect the integrity and security of the ICS Domain and will consider that their actions have the potential to jeopardize the entire ICS system before taking such action(s).
- H. Administrators agree that the use of the Administration account is only for those actions which require that privilege level.
- I. Administrators understand and agree that they may not delegate their administration authority to other Administrators, unless such delegation is specifically approved by the ESOC and the Administrator has signed this DAUP.
- J. Administrators agree that they will comply with ICS Change and Configuration Management requirements found within the "ICS Operations and Policies Manual" located at the Idaho Consolidated Services Team SharePoint site and will apply standard naming conventions to objects in their Organizational Unit hierarchy also located at the Idaho Consolidated Services Team SharePoint site.
- K. Administrators understand and agree to respect the rights of the domain users, integrity of the system, related physical resources, and intellectual property.
- L. Administrators understand and agree that they will cooperate with the OCIO, ITRMC, and/or the ESOC to investigate potential unauthorized and/or illegal use of the ICS Domain.

V. ICS Domain Requirements of Administrators

All Administrators, subject to this DAUP, will:

- A. Attend periodic meetings of ICS Administrators and participate in mailing lists;
- B. Provide the following information to Enterprise Domain Administrators when suspecting problem(s) stems from a change to the Active Directory configuration:
 - 1. Event Description;
 - 2. Account name of affected object;
 - 3. Logon name of affected user;
 - 4. Time of event;
 - 5. Relevant warnings and errors in event logs; and
 - 6. Relevant warnings or errors displayed on screen.
- C. Coordinate any software which interacts with Active Directory or the ICS Domain in any context with the ICS Domain/Enterprise Administration;
- D. Ensure the separation of his/her normal user account with his/her Organization Unit Administration account. The Organizational Unit Administrator understands that it is against policy to add his/her normal user account(s) into the Organizational Unit Administrators group and agrees not to do so;
- E. Create separate Administrator-only accounts for any other Administrators, and will not create Administrator-level accounts in any other Organizational Unit than the Local Administrators' Organization Unit;
- F. Coordinate all new Group Policies with the OCIO ICS Domain Administration Team so as to ensure the proper placement of Group Policies content (scripts, etc.);
- G. Not create mailboxes in other than as-assigned mailbox databases;
- H. "Pre-create" computer accounts in the proper Organizational Units before joining computer accounts to the ICS Domain to ensure those accounts get created in the proper area;
- I. Agree to the following rules when creating Service Accounts:
 - 1. Service Accounts can be created for use in starting and working with services;
 - 2. Agency three-letter agency designator must precede the account name and the letters "SVC" must complete the account name; and
 - 3. Use best judgment with the middle portion of the account name so that a cursory observation of the name will generally intimate the purpose of the account.

For example, Division of Vocational Rehabilitation has an agency designator of "DVR" and the service account will be used for backup services. A possible service account will be "dvrbksvc". Tax Commission's SQL service account: "taxsqlsvc," etc.

VI. Prohibited Activities

Unless expressly agreed to by ITRMC or the ESOC in writing, the following activities are specifically prohibited by Administrators:

- A. Sharing logon credentials with another User or allowing access to the Organizational Unit Administrator account in any way.
- B. Activities that disguise or attempt to disguise Administrator's identity or the identity of his/her account or machine he/she is using, or impersonation of or attempt to impersonate another person or organization.
- C. Interception of, monitoring, forging, altering, or destroying, or attempts to do the same, another User's communications.
- D. Administer the ISC Domain in a way that (a) disrupts, adversely impacts the security of, or interferes with the legitimate use of any computer, the State network or any network that the State connects to, or (b) takes any action that is likely to have such effects. Such conduct includes, but is not limited to: hacking or spamming, placing of unlawful information on any computer system, sending "broadcast" messages to lists or individuals, or any other use that causes congestion of any networks or interferes with the administration of the ICS Domain.
- E. Attempts to bypass network security mechanisms, including those present on the State Network, without the prior express permission of the owner of that system.
- F. Use of an Administrator account as a standard User account.

VII. Monitor and Review of the ICS Domain

- A. The OCIO will monitor and review changes to ICS Domain to ensure only authorized changes occur.
- B. The OCIO reserves the right to monitor and/or review any transmissions sent or received through the State Network by Administrators. Access to other transmissions sent or received through the State Network may occur in the following circumstances:
 - 1. In accordance with generally accepted, network-administration practices;
 - 2. To prevent or investigate any actual or potential information security incidents and system misuse, if deemed necessary by authorized personnel;
 - 3. To investigate reports of violation of local, state, or federal law;

3. To comply with legal requests for information (such as subpoenas and public records requests); and
4. To retrieve information in emergency circumstances where there is a threat to health, safety, or state property involved.

VII. Penalties for Violation of the DAUP

- A. Penalties for violating the DAUP may include, but are not limited to the following:
 1. Restricted access or loss of access to the ICS Domain or State Network;
 2. Potential disciplinary action by the agency employing the Administrator;
 3. Contractual action, such as breach, damages, or termination, when the Administrator is the employee of a contractor, vendor, or other outside entity or partner; and/or
 4. Civil and/or criminal liability.
- B. The OCIO, in consultation with its legal counsel, may contact local or federal law enforcement authorities to investigate any matter at its sole discretion.

IX. DAUP Updates

The ESOC reserves the right to update or revise this DAUP or implement additional policies in the future. All Administrators are therefore responsible for staying informed by attending periodic meetings of ICS Administrators, participating in mailing lists, checking status boards, and complying with applicable ITRMC policies. Any modifications of this DAUP shall be effective immediately upon approval by the ESOC or ITRMC. Current versions of this policy can be found at: <http://cio.idaho.gov/messaging/>

X. Additional IT Acceptable Use Policies

- A. Additional policies related to the acceptable use of other IT systems and services within the State Network can be found at: <http://itrmc.idaho.gov/resources.html#policies>
- B. In addition to adhering to the requirements of this DAUP, Enterprise Domain Administrators must also adhere to the requirements found in Idaho Consolidated Services Policies Admin Annex.
- C. List of Applicable Policies:
 1. ICS Policies_final_02_24_2009
 2. ICS-Policies-Admin-Annex-03-05-2010.docx

XI. Contacts

Subject	Contact	Telephone	E-mail
Policy Questions	Carla Casper	208-332-1853	carla.casper@cio.idaho.gov
Report a Violation	Carla Casper	208-332-1853	carla.casper@cio.idaho.gov
Security Consulting	Terry Pobst-Martin	208-332-1851	terry.pobst-martin@cio.idaho.gov
ICS Help Desk		208-332-1503	helpdesk@cio.idaho.gov

AGENCY NAME: _____

By: _____ Date: _____
Agency Organization Unit Administrator

By: _____ Date: _____
Agency Administrator/Bureau Chief

DEPARTMENT OF ADMINISTRATION

By: _____ Date: _____
ESOC Authorized Representative