



IDAHO CONSOLIDATED SERVICES POLICIES

1. Employee Electronic Mail and Messaging Use

The Idaho Consolidated Services (ICS) System will follow policy P1040 (Employee Electronic Mail and Messaging Use) set forth by the Information Technology Resource Management Council (ITRMC).

2. Naming Standards

Distribution lists, e-mail addresses and resources will all have a standard naming convention and an agency designator associated with it.

- User Accounts
- Global Distributions Lists
- Meeting/Conference Rooms
- Computer Naming Standards
- Server Naming Standards
- Duplicate Name Hierarchy and Standard
- Alias

Refer to “Standard Naming Conventions” document available at

http://cio.idaho.gov/products_and_services/consolidated_messaging_project.htm

3. Restore and Back-up

The backup and restore policy for ICS System will be as follows:

The primary purpose of Exchange Store backups will be for catastrophic system recovery. Additional requests will be considered on a case-by-case basis

All consolidated e-mail servers will have a nightly full backup performed. Those backups will be retained for a period of sixty (60) days.

- Individual Message Recovery: Individual users can restore deleted items for 14 days. The OCIO will not recover individual messages for the customer.
- Individual Mailbox Recovery: Mailboxes can be reconnected by the customer for up to 14 days. The OCIO will not recover individual mailboxes for the customer.
- Archiving and Management of PST Files: The OCIO will not provide archiving services at this point in time. Archiving and the use of PST files are the responsibility of the

customer. It is recommended that the customer establish and enforce policies around archiving procedures. Records retention is the sole responsibility of the participating agency at this point in time. Assistance with consulting, installing, and configuring archiving solutions will be provided by OCIO.

4. Secured and Permission Level Access

- Global Distribution Lists: Enterprise distribution lists access will be limited to select individuals and groups.
- Agency Resources (rooms, equipment, computers, servers, network accounts, applications, etc): Access to agency resource accounts will be controlled and managed by the Agency OU Administrator(s).
- Agency Distributions Lists: User email access to agency distribution lists will be controlled and managed by the Agency OU Administrator(s).

5. Confidentiality Statement

Including a confidentiality statement tagged to each user's messages will be the responsibility of the agency. System level settings are not available to accommodate the various different agency confidentiality requirements. Confidentiality statements can be included by utilizing the client-side signature configuration.

6. Mailboxes

Mailboxes will be created with limits as follows:

- A Standard Mailbox will be at 250 MB. Agencies can choose to upgrade a user's mailbox capacity to 500MB, 750MB, or 1GB. There will be a fee associated with these upgrades.
- ICS will prohibit the sending and receiving of messages with more than 100 recipients and any message (including attachments) larger than 30MB. *(Note: a server-side distribution group is considered as one recipient)*
- Mailboxes will normally be viewable on the Global Address List. If a mailbox should not be viewable on the Global Address List, the agency may choose this option.

7. Active Directory

- Documentation of Changes: a change management process is currently being developed by a multi-agency team.
- Delegation and auditing of Administration Access.
- Attributes

Various design documents exist developed by the Active Directory technical team. Any of these documents are available upon request.

8. Public Folders

A top level public folder will be created for each agency, if requested. Under the top level public folder, additional sub folders can be created by the agency's OU Administrator.

Each agency's Public Folder will have a limit of 5 GB.

It is at the agency's discretion to determine how public folders can be utilized and to what extent it can be utilized by their users. Public folders are not to be used as a repository of individual user information. Public Folder should NOT contain any confidential information such as social security numbers, case record information that is required to be protected, HIPPA information, etc.

Permissions will be set such that only an Agency's users will have access to their public folder tree.

9. Mobile and Web Access

The ICS will support mobile and web access to the system. However, technical support of mobile devices is the responsibility of each agency.

Blackberry Enterprise Server(s) will be provided for agencies with existing Blackberry devices for an additional fee. New Blackberry implementations will be considered on a case by case basis as system resources are limited.

Active Sync for state owned Smart Phones and PDA devices will be enabled.

POP and IMAP will not be enabled protocols in the Exchange Organization.

Outlook Web Access will be enabled for access from the Internet. The address to access Outlook Web Access is <https://owa.ics.idaho.gov>.

10. Third Party Applications

The ICS will support an agency's third party applications that are dependent upon e-mail. This will be done on a case-by-case basis to meet the needs of agencies.

11. Security

State of Idaho staff will be able to authenticate into the network at any Idaho facility.

Only authorized users will be able to log onto workstations and access local/network resources. All authorized users will be uniquely identified and user credentials will not be shared between users.

Information will be accessible across organizational and geographic boundaries, permitting access when staff are travelling, working at home, or on cross-agency collaboration efforts

- **Encryption:** Prior to FOC, the State of Idaho will establish a statewide Certificate Authority. The State would then manage and issue certificates to agencies as needed for SSL and e-mail encryption. *Email certificates will be used to secure email messages sent within the Exchange organizations, and, observing proper key and certificate exchange procedures, external to trusted external organizations..* Certificates will not be issued to non-state entities except for *external entities (such as contractors) as required for secure communications with state employees.* Other technologies will be researched for encrypted external communications.
- **Spam, Virus and Content Filtering:** The Exchange Organization will have multiple layers of virus protection. Initial spam, virus and attachment filtering will be handled by the mail relay server/appliance before reaching the Exchange Organization. Messages will be automatically scanned for spam and viruses. The ICS will drop any message at that percentage which is, given current circumstances, will eliminate dangerous viruses and spam e-mails while minimizing false positives. Agencies will be responsible for screening their own messages that are quarantined by the ICS. The front end servers will perform another layer of virus detection for SMTP mail. The back end servers will also contain virus protection. Finally, all desktops will have an anti-virus included in their end-point protection.
- **Password Policies:**
 - General Overview: A network password is still the first line of defense in protecting an individual's computer, network resources and the information contained in those. Since hackers or insiders will always look for the weakest security link, a weak password is always a benefit to them and a significant detriment to security the entire network.
 1. Must be at least 8 characters in length. (Longer passwords or pass phrases are strongly encouraged)
 2. Cannot contain the user's USERID.
 3. Three out of the following four are required
 - i. Must have upper case letters (A-Z)
 - ii. Must have lower case letters (a-z)
 - iii. Must have at least one number (0-9)

- iv. Must have at least one special character (! @ # \$ % ^ & * () [] { }, etc.)
 - 4. Must be creative and unique
 - 5. Password must meet complexity requirements.
 - 6. Passphrases should be considered and are normally very secure if they also meet the above difficulty factors
 - 7. Administrator accounts will have pass-phrases instead of "passwords" consisting of at least 15 characters.
- Password Change Requirements: Passwords must be changed on a regular basis as an additional measure to ensure that others are not able to see part of a password, or even crack part of it, and eventually obtain the entire password. The following schedule will apply, though agencies may reduce the time required for a change if they have higher security needs:
 - 1. Users must change their passwords at least every 90 days.
 - 2. System administrators must change their passwords at least every 45 days.
- Password Protection Requirements: Creating a strong password that's easy to remember and difficult to guess is not that difficult. However, the effort is wasted if we don't make the extra effort to protect the password. Users should follow these rules to protect their passwords:
 - 1. Never reveal a password over the phone or in an email.
 - 2. Don't give hints about your password's composition.
 - 3. Don't reveal your password for surveys, questionnaires, or any other such purpose.
 - 4. Don't use the "Remember Password" feature.
 - 5. Don't use your network password for other systems.
 - 6. If a password must be written down (strongly discouraged) it must be securely locked or stored in a location to which only the user has access.
- **Account Lock-Out Policy**: Incorrect attempts at logging in may indicate an attempt to break into a network using an employee's user account. In order to prevent this, the account will be locked out after five incorrect attempts to log in. Users who are locked out can be unlocked by their administrators, or may wait fifteen minutes for the account to be open again. Logs will be checked regularly for any evidence to regular administrator account lock-outs to identify possible password hacking attempts.

- **Screen-lock Policy:** Desktop computers are the entry point into the State's Enterprise systems. The Enterprise systems provide the individual with access to both private and sensitive information in addition to the data located on the computer's hard drive. While all users should screen-lock their computers whenever they leave their desks, many employees forget.

All desktop computers shall be configured to have a password-enabled screen saver set to no greater than 20 minutes. This security-lockout feature shall automatically initiate after the desktop computer remains idle from user interaction. The user must then reenter their password to gain access to the computer. This 20 minute policy may be modified for those computers which are used regularly for presentations: the change should only be made during the presentations; the computer must be attended at all times by the individual logged in for the presentation.

- **USERID Re-enter Policy:** Having a computer system remember entered security information, such as a USERID or password is an inherent security risk. Therefore, whenever a user logs off his computer, the USERID will not be "remembered" by the computer, requiring users to re-enter both their USERID and password every time they log in. This does not mean the USERID must be re-entered to unlock the computer after the computer has been screen-locked.
- **General E-mail Security Requirements:** State e-mail is a tool for business communications. Users have the responsibility to use this resource in an efficient, effective, ethical, and lawful manner. E-mail communications must comply with all applicable laws, regulations and generally accepted business etiquette. In this regard, the following requirements are applied:
 - The primary purpose of electronic mail is to conduct official business. Employees may occasionally use electronic mail for individual, nonpolitical purposes on their personal time, if such use does not violate the terms and conditions of this policy or interfere with State business.
 - All e-mail accounts maintained on the e-mail systems are the sole property of the State of Idaho. The agency has the right to monitor any employee's e-mail account. Any unauthorized or inappropriate use discovered during such monitoring activities shall be formally reported to department management for determination of appropriate action.
 - Users should not expect their e-mail communications, documents, or other information to be private and should not use the e-mail system for matters that are not intended for public disclosure. Confidential matters, permitted by law, should be so marked and include a warning regarding accidental transmission to a third-party.
 - E-mail messages are considered State property and may constitute official records of the State of Idaho, and are subject to existing document retention

and public records policies. Sending data via e-mail is the same as sending correspondence on official memo or letterhead.

- Use of the e-mail system as described below is **strictly prohibited**. Users who receive such information should not forward or respond to it, but should immediately report its receipt to their supervisors for proper disposition.
 1. Knowingly or intentionally creating, publishing, transmitting, and/or exchanging messages that are inappropriate, offensive, harassing, obscene, or threatening;
 2. Creating or distributing e-mail containing defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material;
 3. Requesting, viewing, or distributing obscene, pornographic, profane, or sexually oriented material;
 4. Violating laws, rules and regulations prohibiting sexual harassment;
 5. Encouraging the use of controlled substances for criminal or illegal purposes;
 6. Engaging in any activities for personal gain;
 7. Distributing copyrighted information without permission;
 8. Distributing advertisements for commercial enterprises, including but not limited to, goods, services, or property unless such advertisements are part of requested vendor information to be used in carrying out State business;
 9. Violating or infringing upon the rights of others;
 10. Conducting business unauthorized by the department;
 11. Transmitting incendiary statements, which might incite violence or describe or promote the use of weapons;
 12. Conducting any non-department supported fund raising or public relations activities;
 13. Exchanging proprietary information, trade secrets, or any other privileged, confidential, or sensitive information that is not authorized;
 14. Creating or exchanging solicitations, chain letters, and other unsolicited e-mail;
 15. Registering to non-State business related list servers without proper authorization.
 16. Subscription to such a service can result in an overload of received messages directly impacting the performance of State e-mail systems;

17. Engaging in any political activity prohibited by law; and
 18. Using the system for any illegal purpose.
- Users may not knowingly or willfully create or propagate any virus, worm, Trojan Horse, or other destructive program code.
 - Individual use of the e-mail messaging systems is subject to monitoring by the respective agency or, upon request by the agency, by authorized Office of the CIO staff.
 - Employees using the e-mail system are deemed to have accepted the responsibilities and obligations imposed by federal, state, and local laws and regulations as well as ITRMC and department adopted policies, procedures, standards, and guidelines.
 1. Users should not pursue, obtain, exchange, or distribute any non-authorized information that could cause congestion or disruption to e-mail systems, such as screen savers, audio, or video clips, or items that would be in violation of any licensing agreement.
 2. Users shall not access another's e-mail system without authorization from that user or that user's supervisor.
 - **Administrator Account Protection:** Stricter security requirements will be followed for all Domain, Schema and Enterprise Administrator accounts. These administrators are required to have background investigations to minimize the potential for an insider breach. Other Best Practices will be followed according to Appendix Z, separate from this policy. Appendix Z will be made available upon request.

12. Business Continuity/Disaster Recovery

By Final Operating Capability (FOC), the ICS Exchange organization will have point-in-time recovery capabilities utilizing Standby Continuous Replication. In the event of a disaster at the hosting site, operational capability will be transferred to the back-up site. Non-critical business functions shall be restored within 5 business days and critical business functions shall be restored within 72 hours.

Fault tolerant storage will be provided for all data.

NOTE: Full Business Continuity/Disaster Recovery to a back-up site will not be available until FOC.

13. ICS Availability

The ICS is available 7 days a week, 24 hours a day, and 99.9 percent of the time, excluding maintenance windows.

Periodically scheduled maintenance operations will occur, which may cause the system to be unavailable. A schedule for weekend maintenance and weekly backups will be emailed to customers. The ICS current maintenance window is Thursday evenings from 7:00 PM through 10:00 PM. Although it is not anticipated that this maintenance window will be utilized every week, it is recommended that customers do not plan necessary business functions during this timeframe. ICS technical staff will send email notification prior to utilizing a scheduled maintenance window. Emergency non-scheduled maintenance will be performed at the discretion of ICS technical staff. As much advanced notification as possible will be provided to customers.

14. Service Desk

Level 1 Service Support is the responsibility of the customer. Level 1 Service will be included for those customers whose IT support is provided by the ADM. Level 2 and 3 Service support will be provided by the ADM.

Level 1 Service: Level 1 Service Support for the local environment includes, but is not limited to, desktop, PDA/mobile device, network and server environments as applicable.

Level 1 support covers desktop applications and hardware, department specific software and management of user accounts

Level 2 Service: Provides more complex support and/or subject matter expertise on application software and/or hardware and is usually an escalation of the call from Level 1.

Level 3 Service: Provides support on complex hardware and network operating system software and usually involves certified systems engineers.

ADM will have Level 2 and Level 3 technicians on-site and available from 7:00 AM to 5:00 PM (Mountain Time) on regular state work days and on-call after hours, weekends and holidays. After hours calls will be answered within 60 minutes. After hours support can be accessed only by customer's IT staff that have been authorized to contact the ADM Service Desk.

All requests will be tracked through a ticket tracking system. This will help measure the performance of the ICS and OCIO as well as ensure that agencies are resolving the majority of their Level I requests per the SA.

When the customer calls in a problem/change, OCIO personnel or contracted support staff will:

- Initiate an incident ticket in the problem/change application.

- Assign a priority (Outages = Emergency). During nights, weekends and holidays, if scheduled, Help Desk staff will help customer prioritize incident severity, and determine if on-call support is needed.
- Resolve and close incident ticket, or forward ticket to the appropriate OCIO second level support or Independent Software Vendor (ISV), or Independent Hardware Vendors (IHV).
- OCIO will notify the customer when the incident/change is escalated to emergency or is resolved.

15. Public Information Requests

Agencies will be responsible for responding to their own public information requests as they relate to electronic messaging. Agencies are encouraged to adopt policies regarding archiving and saving of messages in order to meet their individual requirements around public information requests.

16. Server Design and Placement

Various design documents exist developed by the Active Directory and Exchange technical teams. Any of these documents are available upon request.

17. Storage Groups and Information Stores

Information Stores and Storage Groups will be managed to best balance performance, security, and recoverability as deemed appropriate by the ICS.

18. Patch Management

Windows/Exchange patches and updates will be applied in a reasonable timeframe after adequate testing has been performed. This timeframe will depend on the urgency for the corrective patch or update. Once patches and updates have been tested, the changes will be implemented.

19. Fax Services

Fax services will be provided. All fax products currently used by the agencies today need to be reviewed and a single product chosen for the consolidated fax service.

20. SMTP Relay Service

ICS will provide SMTP relay services for specific devices and applications. Agencies will submit requests for relay services to the change management board.

21. Contacts

Agency OU Administrators can create contacts per OU, but hidden from the global access list.

22. Hardware/Software Management

Hardware for the ICS will be leased on a three-year refresh cycle.

Software will be on a four-year refresh cycle or based on the recommendations of the vendor.

23. Network

Network connectivity to the ICS is the responsibility of the agency.

24. Accessibility

No configuration on the Exchange Server will be made that will prevent use of speech recognition software allowing persons with disabilities access to their e-mail, voice mail, calendar, etc. and meet the Title V standards of the Rehabilitation Act.