

9300-P168 – Security Controls for Instant Messaging

I. PURPOSE

This document establishes policy for the use of instant messaging (IM) within State of Wyoming agencies.

The use of instant messaging and similar collaborative tools can be of great value to Wyoming agencies but improper and unregulated use of these tools can lead to security breaches, loss of confidentiality, loss of intellectual property, loss of public confidence, and has the potential for litigation.

This policy does not require the use or support of IM communications within an agency's area of responsibility.

II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as agencies).

III. POLICY

- A. Acceptable use of instant messaging technologies shall be governed by Policy 1200-P142 – User Responsibilities. IM shall be used for official state business related communications and limited incidental personal use. Agencies should determine appropriate levels of IM use for their business needs.
- B. Agencies shall inform personnel using instant messaging that their use of IM can and will be monitored at the discretion of the State, and all IM communications using State resources are the property of the State of Wyoming. There shall be no expectation of privacy for personnel using IM on State owned computers. All communicating parties should be aware that both sides of the communications can be monitored, recorded and could be considered public records under the State of Wyoming Public Records Act (WS 16-4-201 et seq).
- C. Users shall save IM sessions in accordance with the State of Wyoming Public Records Act.
- D. User Id logins shall be limited to business account names.
- E. Agency IT staff are authorized to install management software on their resources to monitor and control IM activity.
- F. Instant messaging software and clients will be limited to those specified in approved standards (Pending 9300-S168). No software regardless of the source may be loaded on devices connected to State of Wyoming networks without prior agency IT Staff approval (see Policy 3200-P161 – Malicious Code Prevention).

9300-P168 – Security Controls for Instant Messaging

- G. To the extent possible, instant messaging technologies shall:
1. Provide warnings for opening of previously unopened file attachments.
 2. Automatically scan attachments with an anti-virus software package in accordance with state policies.
 3. Have no ability for running scripts or commands on the clients.

CIO Approved Date: 1/5/2011