

1200-P142 – User Responsibilities

I. PURPOSE

This policy establishes user responsibilities related to information technology (IT) access privileges.

Access privileges to State information and IT resources (as defined in the *Glossary of Information Technology Terms*) come with user responsibilities. Acceptance of these responsibilities is a condition of employment and is required for initial and continuing access to State information and IT resources.

II. SCOPE

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

III. POLICY

- A. Users shall be responsible and accountable for their activities on State IT resources. They shall not violate, aid, abet, or act in conspiracy with others to violate State policies or procedures and applicable State and Federal laws or regulations.
- B. Users shall be continuously aware that all credentials (e.g., the combination of UserIDs, passwords, and/or access tokens) that allow access to any State information, data, or system are explicitly the property of the State of Wyoming and shall only be used for conducting official business.
- C. Each user is responsible for protecting the credentials assigned to him or her and shall not share these credentials with anyone else. If credentials are compromised, lost, or stolen, the user shall immediately report this to a supervisor and to agency IT staff to avoid unauthorized access or misuse. Application specific credentials may be shared with system maintainers but the password must be immediately changed after maintenance is complete.
- D. Users may use the same password on internal systems, network devices, or applications, but shall not use their internal password for external systems, such as for accounts on an external web site, as these systems may not protect passwords in an acceptable manner.
- E. Users shall be responsible for helping maintain the security of IT resources and protecting them from unauthorized access and malicious software, such as viruses, Trojan horses, worms, and spyware. Users shall be suspicious of unexpected file attachments. Users shall consult their IT staff for appropriate precautions to take when confronted with suspicious attachments.
- F. A supervisor and agency IT staff shall both be contacted as soon as possible if users suspect a security policy violation, system intrusion, virus or other malicious software on a State system as detailed in Policy 9400-P190: Reporting Security Events and Vulnerabilities.

1200-P142 – User Responsibilities

- G. Users shall be responsible for protecting data from potential loss by saving it to recoverable storage location or media as instructed by their IT staff, or dictated by agency policies or procedures.
- H. Users shall have no expectation of privacy when using State-owned IT resources. Accordingly, users shall not have an expectation of privacy in anything that they create, place on, store, send, or receive on any State-owned IT resources. Refer to State of Wyoming Personnel Rules.
- I. Users shall not violate copyright laws and must abide by the terms and conditions of the applicable copyright law. Violations of copyright law generally include but are not limited to illegally copying, distributing, downloading, and/or uploading information from the Internet (or any electronic source). Examples of commonly copyrighted items are audio materials, movies, videos, software and images.
- J. Users shall abide by applicable agency, State, and Federal policies, laws, rules, regulations, standards, and procedures pertaining to information security, confidentiality, and privacy when handling information owned by or entrusted to the State. Users shall respect others' privacy when handling their personal information and shall take appropriate precautions to protect restricted information, especially when transmitted or received via computer networks and all other communication devices.
- K. Users shall follow established policies, standards, and/or procedures for the security of restricted information that is stored or transmitted outside of the State or agency's control. (See Policy 9400-P175: Mobile Computing and Telework.)
- L. Personnel shall keep all restricted information out of plain sight and shall not leave it displayed in any form when it is not being used. Workstations shall be locked or unattended displays shall have password protected screen savers enabled in accordance with standards. (See Policy 9400-P173: Logical Access Controls on Information Technology Resources.)
- M. Users shall not disclose restricted information or other State information entrusted to their safekeeping, to anyone not authorized to receive such information.
- N. Each agency shall develop a process to obtain a signed acknowledgement from users that they have read, understand, and will comply with this policy. This signed acknowledgement shall be obtained as a condition of access authorization and shall be maintained by the agency according to their records retention schedule.
- O. Failure to adhere to the responsibilities and accountabilities identified in this policy and the supporting standards or procedures, can result in removal of access privileges, disciplinary actions leading up to or including termination of employment, and/or legal prosecution.

CIO Approved Date: 1/5/2011