State of West Virginia Office of Technology Policy:
Account Management

Issued by the CTO

1.0 PURPOSE

This policy will establish a standard for the administration of computing accounts that facilitate access or changes to State of West Virginia (State) Executive Branch data. This policy will also establish standards for creating, issuing, removing, monitoring, and managing employee accounts.

2.0 SCOPE

This policy applies to all departments (including agencies, boards, authorities, and commissions) within the Executive Branch of West Virginia State Government, excluding constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education using contractor services. However, the West Virginia Office of Technology (WVOT) recommends that all agencies - including those excluded above - follow this procedure.

3.0 POLICY

3.1 The WVOT is responsible for adding, modifying, and deleting network users' account access for Executive Branch agencies. Name changes, accounting changes, and permission changes are all documented.

3.2 All accounts must include a written and authorized Network Logon Request Form, with proper approval documented. User accounts will not be activated until the authorization process and required documentation is completed.

3.3 The WVOT will issue a unique account to each individual authorized to access a particular networked computing and information resource and will promptly deactivate accounts when necessary. (See WVOT-PR1010 – "Account Management" for more information.)

3.4 When establishing accounts, standard security principles of "least privilege access" to perform a function must always be used, where administratively feasible.

3.5 Each agency must have a documented process for periodically reviewing existing accounts to ensure that access and account privileges are proportionate with job function, need-to-know, and employment status. WVOT reserves the right to perform audits on an ad hoc basis. (See WVOT-PO1008 – "Information Security Auditing Program" for more information.)

3.6 Each Executive Branch agency will appoint one (or more) employee(s) to serve as a designated approval authority. This individual(s) will authorize all access modifications for that agency and must complete a Network Logon Request Form, which can be obtained by either contacting the WVOT Service Desk at 304-558-9966 or by email at: servicedesk@wv.gov.

3.7 Agencies must monitor and regularly update approval authorities.

3.8 Those responsible for access to systems/applications/servers, etc. protected by high-level super-passwords (or the equivalent) must have proper auditable procedures in place to maintain custody of those "shared secrets" in the event of an emergency and/or should the super-password holder become unavailable. These documented procedures, which must be appropriately secured, should delineate how these passwords are logically or physically accessed as well as who in the chain-of-command will become responsible for access to and/or reset of the password.

3.8.1 When the employee status of personnel who have access to super-passwords changes, the passwords **must** be changed. Changes in employee status include, but are not limited to: termination, resignation, retirement, and change of departments or agencies.

3.9 Temporary accounts (those used by contractors, vendors, interns, etc.) will be granted on a need-to-use basis following the principle of least privilege.

3.10 Temporary accounts will contain an expiration date of one year or the work completion date, whichever occurs first.

3.11 All temporary accounts must be sponsored by the appropriately authorized member of the administrative entity managing the resource.

3.12 All temporary accounts must be designated as such, so users of those accounts cannot be mistaken for full-time state employees.

3.13 Use of shared accounts is not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares).

3.13.1 Exceptions will require documentation to justify the need for a shared account. It should include a list of individuals who have access to the shared account. The list will be reviewed at appropriate and documents intervals.

3.13.2 The system owner is responsible for the documentation, and a copy will be shared with WVOT.

3.13.3 The documentation must be available upon request for an audit or a security assessment.

3.14 Application and System Standards

3.14.1 Where technically or administratively feasible, shared ID authentication must not be permitted.

3.14.2 Authentication should take place external to an application, i.e., applications should NOT implement their own authentication mechanism. External authentication services should be relied upon.

3.14.3 Passwords must not be stored in clear text.

3.14.4 Role-based access controls should be used whenever feasible, in order to support changes in staff or assigned duties.

3.14.5 Where technically or administratively feasible, systems should allow for lock-outs after a set number of failed attempts. Lock-outs should be logged unless the log information includes password information.

3.15 Email Identification

3.15.1 Where technically or administratively feasible, agencies may require Agency Identifiers in an email address account. An Agency Identifier is a 3-5 letter acronym representing the Agency's name.

3.15.2 Agencies may request an Identifier added to email addresses, in a format approved by WVOT, when:

3.15.2.1 Employees transfer OUT of the requesting Agency to the employment of another agency within West Virginia state government;

3.15.2.2 Employees transfer IN to the requesting Agency from the employment of another agency within West Virginia state government;

3.15.2.3 A new employee email account is created; or

3.15.2.4 In order to standardize all agency email accounts.

4.0 RELEVANT MATERIALS/DOCUMENTS

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws
- WV Code § 5A-6-4a
- WV Executive Order No. 7-03
- WVOT Policies Issued by the Chief Technology Officer (CTO), www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

5.0 ENFORCEMENT & AUTHORITY

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the **West Virginia Division of Personnel**. Please review the **WVOT Policy and Procedure Policy #1000** to review additional provisions concerning enforcement and policy authority.

6.0 POLICY-SPECIFIC DEFINITIONS

6.1 Access– The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.

6.2 Access Controls – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

6.3 Authentication – The process of verifying the identity of a user.

6.4 Procedure – A defined series or sequence of steps followed in a definite regular order ensuring the consistent and repetitive approach to actions.

6.5 User – A person authorized to access an information resource.

7.0 Change Log History

- January 30, 2015 –
  - Changed Section 3.1 to read, "The WVOT is responsible for adding, modifying, and deleting network users' account access for Executive Branch agencies. Name changes, accounting changes, and permission changes are all documented."; Deleted repetitive Section 3.5, "The use of shared accounts is prohibited, unless authorized by the WVOT. Each account must have a designated owner who is responsible for the management of access to that account and for maintaining a list of individuals who have access to the shared account."
- July 1, 2015 –
  - Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions;
- 9/1/2016
  - Added sections 3.12- 3.15
- 10/20/2017 – Policy reviewed. No edits made.