



## Albany State University Password Security Policy

### PURPOSE

To establish a standard for creation and use of passwords, the protection of those passwords, and the frequency of change for such passwords to prevent compromise of confidential information.

### POLICY

***Passwords are a primary means to control access to systems and should therefore be selected, used, and managed to protect against unauthorized discovery or usage.*** ASU maintains electronic information resources which are essential to performing University business. Similar to any other capital resources owned by the University, these resources are to be viewed as valuable assets over which the University has both rights and obligations to manage, protect, secure, and control. University employees, students, and other affiliates are expected to utilize these resources for appropriate purposes, protect access to them, and control them appropriately. Examples of information resources include computer systems, network systems, and data.

### SCOPE

This policy applies to all individuals associated with Albany State University (hereinafter referred to "ASU"), including

- faculty
- staff
- students
- student assistants
- contractors
- temporary staff

This policy applies to the all University-owned information technology hardware, including desktop workstations, departmental servers and institutionally available resources, such as

- mainframes
- servers
- personal computers
- network systems
- access card systems
- computer integrated telephony
- other technology hardware

The policy applies to all University data, and reports derived from University data; and it applies to all programs utilizing University operational data.

### Responsibilities of Information Security Officers

The Chief Information Officer is responsible for ensuring that Albany State University has adequate information security and that this policy is observed. To that end, the Information Security Officer, as designated by the CIO, has responsibility for developing and publicizing the information security policy, and monitoring its compliance. The Information Security Officer coordinates the standards, procedures, and guidelines necessary to administer access to University information resources. The Information Security Officer works in conjunction with information resource owners, the University Data Administrator, and functional users to develop this material.

As expected, every employee, student and affiliate at Albany State is responsible for protection of University assets, including information systems equipment and data. Each employee, student and affiliate at Albany State is responsible for



notifying the Information Security Officer whenever he or she observes actions which seem to be contrary to this policy. The Information Security Officer is responsible for responding appropriately to actual or perceived breaches by working together with the resource users and the Information Technology personnel directly responsible for the resource in question.

## **STANDARD**

This standard applies to all systems and applications used to process, store, or transfer data with a security categorization of MODERATE or higher. These systems include, but are not limited to:

- BANNER
- PeopleSoft
- Kronos
- System-Level servers
- Active Directory (ASU Domain and email accounts)

### **A. Password Construction**

Strong passwords or strong authentication mechanisms must be used. See the Appendix for guidelines on creating a “strong” password.

### **B. Password Protection**

1. **Password shall not be written down for any reason.** The user should strive to choose a password they can remember.
2. **All system-level passwords** (e.g., root, enable, NT admin, application administration accounts, etc.) **shall be changed every sixty days.**
3. **All user-level passwords** (e.g., email, web, desktop computer, etc.) **shall be changed every forty-five days.**
4. User accounts that have system-level privileges granted through group memberships or programs should have a unique password from other accounts held by that user.
5. **Passwords should not be inserted into email messages or other forms of electronic communication.**
6. Users should not use the same password for ASU accounts as for other non-ASU access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, users should not use the same password for different ASU access needs. For example, a user should select one password for the Banner systems and a separate password for PeopleSoft systems. Also, a separate password should be selected to be used for operating system accounts. The exception to this is where a Single Sign On System (such as a portal) may control multiple systems.
7. **Users should not share ASU passwords with anyone, including administrative assistants or secretaries.**
8. **All passwords should be treated as sensitive, confidential information.** Users should not write passwords down and store them anywhere in their office. Nor should they store passwords in a file on ANY computer system (including Personal Digital Assistants or similar devices) without encryption.



9. **Users should not use the "Remember Password" feature of applications.**
10. If an account or password is suspected of being compromised, the incident should be reported to the appropriate access administrator and the user should change the password.
11. Security administrators should perform periodic, random password audits via automated tools or guessing. If a password is determined during one of these scans, the user will be required to change it.
12. **User Should Not Employ Any Automatic Log-In Actions**
13. ASU information system users should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.

#### **C. Password Sharing Prohibition**

Besides the authorized user, passwords should never be shared or revealed to anyone. Temporary or "first use" passwords should be changed the first time that the authorized user accesses the system. Failure to change a temporary or "first use" password leaves the authorized user liable for all actions performed under the assigned account. If users need to share computer resident data, they should use approved network services or any other mechanisms that do not infringe on any policies.

#### **D. Mandatory Change of Password:** If any of the following events occur, a change of password will be mandatory:

1. Unauthorized password discovery or usage by another person
2. System compromise (unauthorized access to a system or account).
3. Insecure transmission of a password, for example via email or instant message. (Even an email transferred via secure Post Office Protocol (POP) or Secure Internet Message Access Protocol (S-IMAP) could be compromised at the Simple Mail Transport Protocol (SMTP) level or read while in your inbox- change the password anyway.)
4. Accidental disclosure of password to an unauthorized person
5. Replacement of account user with another individual requiring access to the same account
6. Password is provided to IT support staff in order to resolve a technical issue (It is strongly recommended that IT support staff request an end-user password as a last resort.)
7. A password is provided to the end-user and the system administrator knows the password. For example, the system administrator provides a new account password or has to reset an account password.

## **GUIDELINES**

### **Application Development**

Application developers should ensure their programs contain the following security precautions:

- Applications should support authentication of individual users, not groups.



- Applications should not store passwords in clear text or in any easily reversible form.
- Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

### **Use of Passwords and Pass phrases for Remote Access Users**

Access to the Albany State University Networks via remote access should be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase. Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks". A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. All of the rules that apply to passwords apply to pass phrases.

## **Procedures**

Procedures for processing password requests strive to balance security requirements and user convenience. These procedures will be followed by Information Technology staff and student workers for all password requests (including new, changed or forgotten passwords) for access to the University's network and e-mail.

1. **Under no circumstances will new passwords be provided by telephone.**
2. The Information Technology staff will be pleased to handle requests made in one of the following ways:
  - Requests may be made in person at Information Technology [James Pendergrast Library, Rm. 323] 8:30 a.m. – 8:00 p.m. Monday-Thursday and 8:30 a.m. – 4:30 p.m. Friday. Photo identification is required.
  - Requests may be faxed to Information Technology at 229-420-1271 8 a.m. – 8 p.m. Monday-Thursday and 8:30 a.m. – 4:30 p.m. Friday. The fax must include a copy of your photo identification and signature.
3. When applicable, confirmation will be sent to user by e-mail or phone when a password change is completed. Please allow 1 hour for password change.
4. A network manager must approve any password change requested by a faculty or staff user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.

## **AUTHORITY, ENFORCEMENT, EXCEPTIONS**

Exceptions must be justified in writing and accepted by the CIO of Albany State University or his/her designee. In the case of an information system managed by a third party, the University CIO can, in concurrence with the information owner, make a determination that the third party's security controls meet or exceed this



standard. This exception must be based on an assessment of the third party's controls and documented in writing.

**Enforcement:**

- Information Technology will, whenever reasonably possible, configure accounts for automatic password expiration and set other options to encourage or remind individuals to change their passwords. IT will do what they can to help individuals to succeed in following the policy.
- Violations of this policy may be referred to appropriate administrative offices for disciplinary action. Violators may be subject to disciplinary outcomes as outlined in the Student Handbook and/or Employee Handbook. In addition to the other sanctions outlined in the handbooks, one possible outcome is the restriction or suspension of access privileges.



## Appendix A

### Guidelines for Creating Strong Passwords

Strong passwords are defined as having the following characteristics:

- Are at least eight characters in length.
- Must contain characters from **at least three** of the following four types of characters:
  - English upper case (A-Z)
  - English lower case (a-z)
  - Numbers (0-9)
  - Non-alpha special characters (\$, !, %, ^, ...)
- Must not contain the user's name
- Must not contain part of the user's full name

Unacceptable Methods to Create a Password:

- Do not use dictionary or actual words. Non-English words are no more secure than English words. (If you accidentally use a tiny dictionary word like "I", "a", "an", or "if" in an otherwise secure password, that is fine.)
- Do not use words or numbers associated with you. Examples include:
  - Social security numbers
  - Names, family names, pet names
  - Birthdays, phone numbers, addresses
- Avoid using your login name or any variation of it as your password. If your login is 'fredrick', do not use substitution or letter reordering. Examples would be 'fr3dr1ck', where the 3=e and the 1 (one)= i. Alternatively, do not use kcirderf (backwards) or add a digit to the beginning or end of the word (1fredrick or fredrick1).
- Do not use the same character for the entire password (e.g., '11111111') or use fewer than five unique characters.
- Do not use common letter or number patterns for your password (e.g., '12345678' or 'abcdefgh').
- Substitution should not be used on common words or with common substitutions (e.g., 3=E, 4=A, 1=l, 0=O, etc).
- When changing a password, change to an entirely new password. Do not just rotate through a list of favorite passwords.

Password cracking tools are sophisticated and are able to crack passwords that are created using these unacceptable methods.