Section 1 General Policies & Procedures

1.1 - Account Compromise Policy & Procedures

Purpose

To clearly define the types and severities of account compromises that may occur in WVUP systems as well as the process for safeguarding these accounts and notifying users.

Information Sources

WVUP IT receives notifications from WV Net if email accounts from the @wvup.edu domain appear on lists of compromised accounts distributed by MS-ISAC (Multi-State Information Sharing & Analysis Center).

Types, Severity, and Procedure

- Direct
    - Evidence exists that a WVUP-maintained account has been compromised.
        - Access logs are maintained and notifications are sent to appropriate Information Technology staff when a suspicious activity is detected
    - Severity
        - High
    - Procedure
        - All WVUP-maintained accounts assigned to the user will be immediately disabled.
        - The user will be notified through alternative methods to resolve
            - Alternate emails listed in Banner
            - Phone number listed in Banner
        - The user will need to change their password from the default. Users shall not re-use passwords.
- Indirect
    - Evidence exists that an account associated with a WVUP-maintained account has been compromised.
        - WVUP receives notifications from REN-ISAC of any third-party accounts associated with WVUP email addresses found in compromised accounts lists
        - Severity
            - Low to medium

- Procedure
  - Inform users of potential compromise through their WVUP-issued email
    - Request that user change passwords immediately
    - Include other pertinent security information
      - Best practices, etc.
  - If the password is not changed within x days, WVUP IT will reset the password and make the attempt to communicate with the student again through the alternative methods listed above.