# ATS Current Security Settings - Last updated: 05/02/2025

## ATS current security:

- Our ATS software is SOC II Type 2 certified and HIPAA compliant.
- The data center we use is SSAE-16, SOC II and FedRamp Certified.
- 2FA or MFA is required for staff and may not be disabled. Authentication apps such as Microsoft, Google & DUO may be used.
- Data is encrypted; in transit using a 256-bit AES SSL encryption.
- Data encryption “at rest” is available for an additional fee.
- All ports use our SSL certificate.
- Each client has their own physically separate database. No data is comingled.
- Each database is backed up daily to an off-site, encrypted, location.
- All data is stored in the United States.
- Administrators can configure:
    - The minimum password length; 12 by default currently.
    - The ability to force password change after # number of days. This is a max of 365 days.
    - Lock user accounts after a minimum of 3 failed attempts; max of 5.
    - The ability to auto-logoff users after a period of inactivity in the ATS Desktop. Inactivity for the web modules are defaulted to 15 minutes.
- User Account Security & Access Controls
    - Password Policy
        - Strong password enforcement is in place, requiring a combination of:
            - Uppercase and lowercase letters
            - At least one number
            - At least one special character
        - Passwords are checked against a restricted list to prevent the use of:
            - Common patterns
            - Personal identifiers such as mascot names, first names, and last names
            - The last four passwords are stored and cannot be reused immediately.
    - Account Recovery

      Security questions and answers are used as part of the password reset process for user and athlete accounts.
    - Authentication Logging

      All login attempts are logged, including IP address capture when available.
    - Audit Logging

      All data entered, viewed, or updated is date-time stamped and associated with the user account responsible.
    - Role-Based Access Controls
        - Team-Based Restrictions: Users may be limited to viewing information for specific teams.
        - Data Permissions: User permissions can be set to control:
            - Visibility of specific information
            - Ability to add or edit content
        - Export/Print Restrictions: User accounts may be restricted from printing or exporting reports.
- Administrators have the ability to force all users to enter a new password.
- Administrators have the ability to force all students/athletes to enter a new password.