SECURITY & COMPLIANCE
HOW SKYWARD PROTECTS YOUR DATA

As a K-12 EdTech partner, Skyward is committed to keeping our customers and products safe from threats. Today's hackers are growing ever more sophisticated, and as a result, we understand the need to continually review and refine our security best practices.

HERE ARE SOME SECURITY MEASURES SKYWARD CURRENTLY HAS IN PLACE.

SECURITY REVIEW

Every year, third-party experts evaluate Skyward's ability to stand up to threats. This annual audit includes vulnerability testing on:

Skyward corporate networks + Skyward applications + Skyward server configurations

Data security measures Skyward has in place:

- Encryption keeps data from being intercepted and read while it is transported on a network.
- Encryption protocols Skyward uses:
  - » Web: SSL (HTTPS)
  - » LDAP: Kerberos/TLS/LDAPS
  - » Email: TLS
  - » SFTP/SSH
- Annual audits using the Center for Internet Security CIS Top 20 Critical Security Controls.

SCC HOSTED DATA SECURITY

Below are just some of the security measures provided by Skyward's secure cloud hosting service:

- SSAE 18 Type II SOC 2 audits completed annually
- Team members CISSP certified
- Certified internal security auditor on the team
- Modern controls in place to ensure physical access to the data centers is tightly restricted. Physical restrictions include:
  - » Access to the data center is controlled with dual-factor biometric credentials.
  - » All entrances to the data centers are either alarmed or monitored.
  - » All entrances to data centers are through "man-traps."
  - » Only authorized employees have access credentials for access to the data centers.
  - » All door access is logged.
  - » Cameras record activity in the data center and the interior and exterior of the facility 24/7.

MULTI-FACTOR AUTHENTICATION

Skyward enhances the security of all its apps and software through the use of multi-factor identity verification. Not only do employees need a password to access our databases, they also need proof of identity through another authentication source such as Office 365 or Google.

For more information on Skyward security best practices, please visit:
https://www.skyward.com/blogs/skyward-insider/2024/september/skyward-security-best-practices

DATA COMPLIANCE

Skyward complies with the data security regulations of both the Federal Education Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA).

Data classification features in Skyward:

- **Data is always encrypted with SSL strong encryption during twransport.** This prevents eavesdroppers from reading private data using man-in-the-middle attacks.
- **Direct database access is restricted and only allowed through a VPN connection to ISCorp's cloud hosting data center.** VPN connections are restricted to authorized district SysAdmin personnel. Direct database connections require authorization and are restricted to district SysAdmin personnel. A typical user account in Skyward does not have direct access permissions within the database.
- **Application features are restricted by security.** Each user in the system is assigned permissions either by role-based security groups or user-based security permissions assigned to individual users. Security permissions define the user's ability to see application menus, which functions they can use, and what data they may view or modify.

Application auditing features in Skyward:

- At a minimum, access to Skyward requires users to provide an authorized user and password. Authorization can be configured to use local accounts, Secure LDAP, or SSO using SAML identity providers.
- Audit logs of user activity include date/time, IP address, and what has been changed. Audit logs are stored with the customer's database and cannot be modified using the user interface.
- ISCorp's secure cloud systems have strict access control on system and server logs.

CERTIFIED SKYWARD STAFF

Our information security team is dedicated to continual learning of best practices. From partaking in ongoing professional development to earning certifications, Skyward staff ensure they are familiar with the latest cybersecurity threats and risks.

Certifications include:

- **Certified Information Systems Security Professional**
  The world's premier cybersecurity certification
- **Comp TIA PenTest+**
  Assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of network against attacks

SECURITY AWARENESS TRAINING PROGRAM

Information Security implemented a security awareness training program to increase all employees' understanding of their responsibilities in protecting the confidentiality, integrity, and availability of Skyward's and our customers' valuable data.

- **Employee Security Awareness Training**
  - » All employees must complete new hire security awareness training within four weeks of their date of hire.
  - » A monthly security awareness refresher training must be completed within 21 days of being assigned.
- **Employee Phishing tests**
  - » A monthly phishing test email is sent to all employees.
  - » Employees that fail 25% or more of their phishing email tests over four months will be enrolled in additional 1:1 remedial training with Information Security. Employees enrolled in remedial training will also receive an additional monthly phishing email test until they improve their failure rate to below 25%.
- **Role-Based Security Awareness Training**
  - » Role-based OWASP Top 10 security awareness training is required for developers whose responsibilities require increased security awareness. Role-based training must be completed by new hires or refreshed periodically, as required by the Information Security team.