Information Security Training Policy

1. Overview

A strong security program requires staff to be trained on security policies, procedures, and technical security controls. All staff need to have the necessary skills to carry out their assigned duties. This policy promotes continuous employee supports around data security and privacy education.

2. Purpose

The purpose of this policy is to ensure security awareness and training controls protect information systems and Personally Identifiable Information (PII) and ensure information availability, confidentiality, and integrity of data.

3. Scope

This policy applies to all Pinnacle Charter School staff.

4. Policy

A. GENERAL

Pinnacle Charter School management is charged with ensuring all Pinnacle Charter School employees are knowledgeable and following best practice protocols for managing data. As such, a high priority is given to effective security awareness and training throughout the organization. This includes implementing a viable information security program comprised of a strong awareness and training component. The Chief Business Officer is ultimately responsible for the security of data and assets of Pinnacle Charter School. The IT Manager in cooperation with senior Pinnacle Charter School management shall ensure that a consistent, school wide, well-supported and effective security program is implemented and maintained.

The IT Manager shall be responsible for developing, implementing, and maintaining a Security Awareness and Training Plan. This plan shall document the process for staff security training, education, and awareness and ensure that all Pinnacle Charter School employees understand their role in protecting the confidentiality, integrity, and availability of data assets. The plan shall cover what information to communicate, when to communicate it, with whom to communicate, responsibility for communication, and the process by which communication shall be effected.

Secondly, the plan shall ensure that staff are provided with regular training, reference materials, supports, and reminders that enable them to appropriately protect Pinnacle Charter School data assets. Training shall include, but is not limited to:

- Responsibilities for protecting sensitive information
- Risks to information assets and resources
- Data encryption and access management
- Secure use of data and information assets
- Pinnacle Charter School information security policies, procedures, and best practices

- Protecting assets and identities

B. TRAINING PLAN REQUIREMENTS

The training plan shall ensure:

- All Pinnacle Charter School users attend an approved security awareness training class within 30 days of being granted access to Pinnacle Charter School resources.
- Staff receive training appropriate for specific job roles and responsibilities. After such training, staff must verify through certificate completion and assessment that he or she received the training, understood the material presented, and agrees to comply with it.
- Staff are trained on how to identify, report, and prevent security incidents and data breaches.
- Appropriate security policies, procedures, and manuals are readily available for reference and review.
- Staff annually attend security awareness refresher training.
- Users sign an acknowledgement stating they have read and understand Pinnacle Charter School acceptable use requirements regarding computer and information security policies and procedures.
- Staff must be provided with sufficient training and supporting reference materials to allow them to protect Pinnacle Charter School data and assets.
- The Chief Business Officer or their designee shall prepare, maintain, and distribute an information security manual that concisely describe information security policies and procedures.
- Cloud computing and outsourcing security awareness training shall address multi-tenant, nationality, and cloud delivery models.
- Staff are aware and accept the risks, responsibilities, and limitations related to the Bring Your Own Device (“BYOD”) Policy.

C. MANAGEMENT IMPLEMENTATION

The Chief Business Officer or their designee shall:

- Develop and maintain a communications process to communicate new security programs and items of interest.
- Ensure that staff responsible for implementing IT Department safeguards receive training in security best practices.
- Ensure periodic security reminders (flyers or posters, emails, verbal updates at meetings) keep Pinnacle Charter School staff up-to-date on new and emerging threats and security best practices. The frequency and method of delivery of such reminders shall be determined by the Chief Business Officer.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Pinnacle Charter School internal operations. Examples of management controls include:

- Documented information security training plan with evidence of consistent update and version control of the document
- On-demand review of existing training program information and implementation within the organization
- Completion and employee acceptance logs for completed education
- Completion rate statistics
- On-demand evidence of continuing education and reminders are in place

4. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

5. Distribution

This policy is to be distributed to all Pinnacle Charter School staff using or accessing Pinnacle Charter School information resources and assets.

6. Policy Version History

Version	Date	Description	Approved By
1.0	12/15/2017	Initial Policy Drafted	