Securing Sensitive Information Policy

1. Overview

Pinnacle Charter School has a responsibility to maintain high standards of security for all electronic information under its control. Data that is stored on or accessed by Pinnacle Charter School assets must be secured against intentional or unintentional loss of confidentiality, integrity, or availability regardless of location.

2. Purpose

This policy protects Pinnacle Charter School information assets and helps ensure our ability to continue business operations for Pinnacle Charter School.

3. Scope

This policy applies to all Pinnacle Charter School staff, users, and contractors who use information resources.

4. Policy

A. GENERAL

Computers, systems, and application must have an identified local Data Owner who is responsible for the data and can act as a point of contact.

Devices shall be either managed and reviewed on an ongoing basis for appropriate security measures by information technology support professional within the IT Department. These reviews shall include adherence to baseline security requirements as well as additional strategies for protecting Pinnacle Charter School information.

B. SECURING ASSETS

The following policies and procedures are to be implemented relating to securing sensitive assets:

- All devices shall have appropriately supervised professional technical support staffing sufficient to maintain information security. Staffing levels should be appropriate to ensure the type of private information for which they are responsible and the level of risk is adequately managed.

- Devices shall be set up in accordance with applicable Pinnacle Charter School information security guidelines and standards.

- Security vulnerabilities are regularly found and publicized for software. Regular patching, installation of newer versions, and other maintenance shall be performed to protect data. Automatic settings or centralized updating of security patches is strongly recommended for most desktop and server based hardware.

- Access to private data shall be authenticated (e.g. by using a strong and complex password) with file access privileges differentiated by user. Administrator or root level passwords should be exceptionally strong. User accounts with fewer privileges should be used instead of root accounts whenever possible. Periodic review of access privileges and account scavenging is required.

- All external transmission across open networks shall require both the authentication data (e.g. user ID and password) and the data itself to be encrypted with strong encryption.

- Encryption of all data stored on laptop computers or other portable devices is required.

- Use of portable flash media is expressly forbidden without prior approval from the Chief Business Officer. Should portable flash media be used, data must be encrypted on the device.

- Pinnacle Charter School computers shall have anti-virus software and/or malware filters installed and updated daily (automatic updates recommended) excepting for devices expressly excluded by Chief Business Officer authorization.

- Physical access to computers shall be restricted to the degree possible when not in use. Devices must be turned off when not in use. Laptops must be physically restrained using typical anchoring devices and servers must be housed in an appropriate and secure physical facility.

- Password protected screen saver programs should be used in all locations and should universally locked. Timeouts shall be set at a minimum of twenty minutes on internal devices.

- Host security log files must be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event (at least 90 days of logs).

- Servers storing sensitive information must be scanned regularly with vulnerability testing software so that corrective actions can be taken should an exploit be found. Desktop vulnerability scans shall be scanned regularly and sent to the IT Manager for review and mitigation if necessary.

- Sensitive information in databases, logs, data files, backup media, etc. shall be stored securely by means of encryption, masking, truncation, de-identification, or other means of blurring identifying features.

- Periodic backup copies of software and data must be made, tested, and stored securely. The physical security of the removable media must be maintained and plans made to allow recovery from unexpected problems.

- A secure deletion program or mechanism shall be used to erase data from hard disks and media prior to transfer, surplus, or disposal of hardware. Permanent media (e.g., CD's, DVD’s, etc) must be physically destroyed.

- Services available on computers or other devices shall be limited as much as possible. Procedures shall exist for component services installed on workstations. Web server, ftp server, mail server, peer to peer, and anonymous file sharing software can significantly raise the security risk to private data.

- Workstation firewalls shall be instituted at the discretion of the IT Manager to further limit malicious desktop intrusions.
- Pinnacle Charter School provided education on data security practices shall be completed for both new and existing employees. Employees working with sensitive information may require additional training.

C. PROTECTING SENSITIVE DATA

One or more of the following additional actions should be used to further protect sensitive information depending upon on the data sensitivity, classification, and requirements:

- Limiting storage of private data to a hardened file server
- Severely restricting the volume and duration of the information stored
- Moving data to a dedicated computer holding no other applications or data
- Limiting network access to a list of specific machines or devices (access control list)
- Using a local non-routed IP address or network which prevents any access either to or from the Internet
- Separating sensitive information from other data and storing that information independently on non-networked devices

D. REVIEWS, AUDITS AND OVERSIGHT

Pinnacle Charter School shall conduct periodic reviews of information systems in their control that contain sensitive information and adjust controls/procedures as appropriate. Each Pinnacle Charter School department is required to document the activities they will conduct to review information systems activity. These activities shall include:

- Regular review of user permissions and roles for those who have been granted access to systems that contain sensitive information to ensure that only those who need access have access to the systems
- Periodic review of Pinnacle Charter School and departmental policies and practices to ensure they address emerging data security trends in the department
- Document the completion of the periodic reviews described above
- Periodic review of audit logs
- Periodic review of user areas to ensure a clear desk for papers and removable storage media and a clear screen at the end of a work day

IT Managers and Systems Administrators shall have the following responsibilities:

- Establishing and publishing server criteria and role to be determined a critical server
- Periodically reviewing critical servers based on established criteria
- Performing and reviewing vulnerability scans of critical servers

- Implementing intrusion detection systems and reviews
- Performing and reviewing ad-hoc scans for security threats
- Monitoring local data security compliance in their individual areas of responsibility

E. PERIMETER CONTROLS AND FIREWALLS

A software firewall, hardware firewall, or other network filtering (e.g. port or IP address filtering) technology must be used to protect against Internet threats and to limit network access to devices storing sensitive information.

- Firewalls shall be installed at each internet connection and between any demilitarized zone (DMZ) and the internal network
- Firewalls shall be installed and active on mobile devices such as laptops and similar devices
- Inbound Internet traffic shall be limited to IP addresses within the DMZ. Firewalls shall not allow direct traffic between a public network and sensitive data
- All exceptions to this policy shall be documented and authorized by the Chief Business Officer or their designee

Firewall documentation shall include:

- Services and ports allowed (inbound and outbound)
- Business need for each service and port
- Information security features to be implemented
- Date of last change
- Exceptions and reasons for exceptions

F. ADMINISTRATION AND MANAGEMENT OF SENSITIVE INFORMATION

The Chief Business Officer shall ensure policies and procedures govern the collection, use, processing, storing, transmitting, and disclosing of sensitive information. The Chief Business Officer shall ensure:

- Policies and procedures are clear, reasonable, and protect Pinnacle Charter School and individuals
- Appropriate consent is obtained before collecting, using, and disclosing PII
- Sensitive information is fairly collected and processed in reasonable, appropriate, and lawful ways
- Requests for sensitive information are processed for limited purposes
- Controls are adequate, relevant, and not excessive

- Information is maintained no longer than necessary and in accordance with applicable federal and state regulations, statutes and laws

- Data requests are processed in accordance with student and employee rights in mind

- Assets and information are transferred only to areas with adequate protection and all assets are encrypted to protect unauthorized access

- Transparency is provided to the public and to parents on the data that is collected, used and shared within

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the Pinnacle Charter School internal application development and release methodology. Various control and documentation examples are provided throughout relevant Pinnacle Charter School operational policies.

6. Enforcement

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

7. Distribution

This policy is to be distributed to all Pinnacle Charter School staff and vendors managing and supporting Pinnacle Charter School systems.

8. Policy Version History

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