No. 823

Palmyra Area School District

SECTION: Operations

TITLE: Information Systems Security

ADOPTED: September 13, 2012

REVISED:

823. INFORMATION SYSTEMS SECURITY

1. Purpose

The purpose of the Palmyra Information Systems Security Policy is to create an environment within the Palmyra Area School District that maintains system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data. The Palmyra Area School District will adhere to the policies identified in this document and use these standards in which to develop, implement, and maintain security. Technological advances and changes in the District requirements will necessitate periodic revisions; therefore, Palmyra Area School District will review and update IT security plans at least annually or following any significant change to its business, computing, or telecommunications environment.

The Palmyra Area School District's increased use of the Internet for conducting official business has generated the following security concerns:

- Information Integrity - Unauthorized deletion, modification or disclosure of information;
- Misuse - The use of information assets for other than authorized purposes by either internal or external users;
- Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users;
- Penetration - Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs;
- Computer Viruses – Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files or devices on a system or through multiple systems in a network, that may result in the destruction of data or the erosion of system performance;
- Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization;
- Component Failure - Failure due to design flaws or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component; and

- Unauthorized additions and/or changes to infrastructure components.

Because information technology security planning is primarily a risk management issue, this policy and its associated standards and guidelines focus on the creation of a shared and trusted environment, with particular attention to:

- Common approaches to end-user authentication;
- Consistent and adequate network, server, and data management;
- Appropriate uses of secure network connections; and
- Closing unauthorized pathways into the network.

The Palmyra Area School District will take steps necessary to initiate an approach to:

- Ensure secure interactions between and among business partners, external parties, and school districts to utilize a common authentication process, security architecture, and point of entry;
- Prevent misuse of, damage to, or loss of District hardware and software facilities;
- Prevent unauthorized use or reproduction of copyrighted material by public entities.
- Ensure secure interactions between the Palmyra Area School District and outside agencies and ensure that there is a shared and trusted environment.

The Palmyra Area School District will:

- Operate in a manner consistent with the District Acceptable/Responsible Use Policy;
- Develop, implement, maintain, and test security processes, procedures, and practices to protect and safeguard voice, video, and data computing and telecommunications facilities (including telephones, hardware, software, and personnel) against security breaches;
- Train staff to follow security procedures and standards;
- Apply appropriate security measures when utilizing transactional Internet-based applications,
- Ensure and oversee compliance with this policy.

Security Policy Scope

For the purposes of this policy, security is defined as the ability to protect the integrity, availability, and confidentiality of information held by The Palmyra Area School District, to protect it's assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of network facilities and off-site data storage; computing, telecommunications, and applications related services purchased from commercial concerns; and Internet-related applications and connectivity.

General Security Policy

It is the network security policy of the Palmyra Area School District that:

1) The Palmyra Area School District will operate in a manner consistent

with the maintenance of a shared, trusted environment for the protection of sensitive data and business transactions. The District will use security protocols (including means of authentication and authorization) relied upon by others; and the integrity, reliability and predictability of the District WAN will be maintained.

2) The Palmyra Area School District will establish its secure business applications within the guidelines of the IU13 Network Infrastructure. This requires that all parties interact with agencies through a common security architecture and authentication process. The Palmyra Area School District will maintain and operate the shared infrastructure necessary to support applications and data within a trusted environment.
3) Furthermore, the Palmyra Area School District will operate its applications and networks within IU13's Network Infrastructure and will subscribe to the following principles of shared security: Follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels; Recognize and support a standard means of authenticating external parties needing access to sensitive information and applications; Follow security standards established for securing servers and data associated with the secure application; and follow security standards established for creating secure sessions for application access.
4) The Palmyra Area School District will address the effect of using the Internet to conduct transactions for business with other public entities, citizens, and businesses.
5) The Palmyra Area School District will ensure staff is appropriately trained in Informational Technology (IT) security procedures. The District will make staff aware of the need for IT security and train them to perform the security procedures for which they are responsible.
6) The Palmyra Area School District will review its IT security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment. Examples of these changes include modifications to physical facility, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization, or budget. Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified by third parties.
7) The Palmyra Area School District will participate in IT Security Policy and Standards Compliance Audit once every three years. The audit will be performed by the PA State Auditor General's office independent of the Palmyra Area School District. The work will follow audit standards developed and published by the State Auditor General. The Palmyra Area School District IT security processes, procedures, and practices may contain information (confidential or private) about the District's business, communications, and computing operations or employees. Policy and procedures for distribution of any related documentation should consider

8) sensitive information and related statutory exemptions for such information from public disclosure.

Maintenance of Policies, Standards, Guidelines and Recommendations
Technological advances and changes in the business requirements of the Palmyra Area School District will necessitate periodic revisions to policies, standards, guidelines, and recommendations. The Palmyra Area School District is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of the Technology Department and Superintendent of Schools.

Security Policy; Review, Schedule and Updates
Technological advances and changes in the business requirements will necessitate periodic revisions; therefore, the Palmyra Area School District will review and update IT security plans at least annually or following any significant change to its business, computing, or telecommunications environment.

If the District purchases IT services from another organization, the District and the service provider will work together to make certain the IT security plan for the service provider fits within the District's security plan. The District will obtain a copy of the service provider's network security plan to determine if it complies with the District Security Plan. If two or more agencies participate with each other in operating an information service facility, the agencies will develop a joint IT security plan which meets their mutual needs.

The Palmyra Area School District will promote security awareness by informing employees, associates, business partners, or others using its computers or networks about security policies and practices, what is expected of them, and how they are to handle the information.

Technology Staff (ITS): Role and Responsibilities
The Palmyra Area School District Technology Staff is responsible for developing and maintaining the District's Security Policy. The Technology Department will:
Develop and maintain the Security Policy
Research the IT industry for security related issues and determine how it affects the District IT infrastructure as a whole
Participate in local and/ or national security organizations for the purpose of sharing security information, pitfalls, warnings, etc.
Work with State Auditor's Office on Security Audits as necessary

The Palmyra Area School District will designate an individual to serve as a contact concerning all security-related issues. This individual will:
Develop and maintain District-specific security policies
Ensure that the District is adhering to State of Pennsylvania Security Policy
Research IT industry for security related issues and how it affects the District specifically

Monitor security issues within the District's IT resources

Facilitate the State Auditor's Office Security Audit

Web Server; Connectivity, Security

If the Palmyra Area School District maintains and houses web servers that reside on the District network and is accessible from the Internet. The district is required to "harden" the server by making sure that all the current operating system patches are applied and kept up-to-date, removing any unnecessary server processes.

E-mail; Functionality, Security, Limitations

For the purpose of security and limiting Spam into the network, the Palmyra Area School District shall require vendors of services to implement and maintain mail relays on the inside of the firewall. All mail must come through the mail relay and be "relayed" to the appropriate mail server.

1) No direct SMTP from the Internet. The District will utilize the mail relays for mail traveling in from the Internet.

2) No POP or IMAP from Internet to mail servers inside the network. The District will utilize a web interface (HTTP/HTTPS) to access this mail.

3) No POP or IMAP from the IU13 network to private mail accounts on Internet. The District will utilize a web interface (HTTP/HTTPS port) to access this mail.

4) Users will be instructed to never open any email attachments on the network except via PASD email. Users will be instructed to use extreme caution when opening email attachments to ensure that the attachment is safe. Virus scanning is used on the district email system.

Antivirus Software; Virus Prevention, Detection and Removal

Palmyra Area School District will:

1) Maintain real-time anti-virus software on the network including all servers and workstations.

2) Be diligent about keeping virus definition files up-to-date.

3) Once a device is infected with a virus, the offending machine should be removed from the network until such time the virus can be removed from the machine.

4) Ensure copies of virus-detection and eradication tools should be kept offline. Otherwise it is possible that the virus could modify the detection tools to prevent its own detection. The network administrator should actively scan/check for viruses online, but periodically use the off-line, trusted copies of the tools to scan the systems.

Firewalls Requirements; Use, Functionality and Port Restriction

IU13 will maintain a firewall within the core of the network that provides one level of protection of the network from the connection to the Internet. Below are examples of what will not be permitted:

No direct SMTP from the Internet. The District will utilize the IU13 maintained mail relays for mail traveling from the Internet.
No POP or IMAP from Internet to mail servers inside network. The District will utilize Web interface (HTTP/HTTPS) to access this mail.

No POP or IMAP from IU13 network to private mail accounts on Internet. The District will utilize a web interface (HTTP/HTTPS port) to access this mail.

No FTP access is allowed from Internet to a device on the district network.

IU13 will not restrict FTP out of the network to a device on the Internet provided that session/transfer is initiated from the IU13 network.

No LAN protocols mapped to and/or from devices on Internet (i.e. NetBios, NetBeui, NFS, etc.).

No outbound port that has the potential of propagating industry-known viruses, worms, etc. will be allowed.

The exception to these port restrictions is when the district has a VPN implemented between them and a third party. In that scenario, all ports are available for use provided the traffic goes through the VPN.

At no time may a district permit a third party entity to connect directly to their local area network behind the IU's firewall. This includes terminating third party circuits behind IU13's firewalls and/or utilizing a PC remote control product (i.e. PC Anywhere).

Non-Educational/District-Business Related Network Traffic
Bandwidth has a high cost associated with its usage. The IU13 network and District network were implemented and are maintained to allow state and district employees to utilize automated systems and tools to help facilitate their carrying out work responsibilities and duties and meeting the needs of those individuals they serve. The IU13 and/or District network infrastructure must not be utilized for personal gain and/or entertainment. Unnecessary applications that pose potential security risks will not be permitted. These include, but are not limited to:

1) Instant Messaging protocols outbound from the District network to Internet will not be permitted.
2) Music/video/file sharing services and any other illegal software or services <u>will not</u> be permitted on District networks. There are legal ramifications that are tied to users who use these applications to share

3) files.
4) Internet streaming of audio and/or video will not be permitted. Users are not to use the PASD network and computers to listen to the radio, watch movies, watch sporting events, etc.

Wireless Access Connectivity
The District will enable and configure encryption on all wireless devices.
No installations of wireless devices, such as wireless access points, wireless printers, wireless network cards may be installed in the district by any person except a member of the IT Services Department. Proper configurations must be performed in order to protect the network.

Consideration for wireless connections will be based upon the need for the connection, as well as assuring security and integrity of the network. Wireless access will be denied for such reasons as, the room is already hard-wired for computers.

Internet Filtering
The District will use the IU13 Internet filtering servers located at the core to provide content filtering for the district. The District will utilize proxy servers for the purpose of tracking Internet usage. The District will be CIPA compliant.

Passwords; Guidelines, Protection of, Bad examples
Passwords are our personal identification keys that allow access to various IT resources on the District's network. Passwords help ensure that only authorized individuals access a computer system, a network device, an application, a file, data, etc. Passwords also help to establish accountability for all transactions and changes made to those IT resources. The District enacts strict password policies in securing our segment of the State network infrastructure and our local network. The following guidelines are used when developing these password policies.

Choosing a Password:
Passwords must contain at least 5 nonblank characters.

Passwords must contain a combination of letters and numbers.

Passwords may not contain the user ID.

Passwords may not include the personal information about the user that can be easily guessed: user name, spouse's name, kid's name, employee number, social security number, initials, pet's name, birthdate, telephone number, city, etc.

Passwords may not include common words from an English dictionary or foreign-language dictionary. Hackers have tools that enable them to break any password found in a dictionary or that is a simple transformation of a dictionary word.

Passwords may not contain commonly used proper names, including the name of any fictional character or place.

Passwords may not contain any simple pattern of letters or numbers such as "qwertyxx" or "xyz123xx."

Passwords should not be trivial, predictable, or obvious.

A complex password that cannot be broken is useless if you cannot remember it and have to write it down. For security to function, passwords must be memorized and not displayed for others to view.

Protecting Passwords:
Do not disclose your passwords to anyone except when there is an overriding operational necessity (i.e., support issue).

Do not leave passwords in a location accessible to others or secured in a location for which protection is less than that required for information that the password protects.

Use Secure Shell (SSH) to avoid sending your password in clear text over the network. Crackers can break into a network, set up a program called a Sniffer that listens to the network for passwords, and steal your password. Anytime you type your password to log in to another computer using telnet, ftp, rlogin, etc., your password can be stolen.

Passwords should be unique to users and users should never share passwords.

Passwords should be changed at least every school year and never reused.

Passwords should be changed if anyone else learns the password.

Never use default passwords. All passwords should be unique. This is especially important for administrator accounts with extended rights.

Passwords should be required on all user accounts.

Do not let support vendors have free reign of the Districts IT resources. If a vendor needs access to some resource for support, give the vendor a password and then change it and lock them out when their support is complete.

Be diligent about removing user accounts for staff no longer employed by the Palmyra Area School District.

Users should log out when leaving their computer, especially administrative users with extended rights.

Teachers and/or staff members may never allow another user (ex. Student) to use their computer while they are logged in the network. Teachers and staff have more privileges than students, such as grade books, etc. and students should never have access to those rights.

Students may never use another student, teacher, or staff member's password nor may they use a computer that is already logged in as another user. If you suspect your password has been stolen or "cracked", notify the technology staff and change it immediately.

Physical Access; Security Guidelines and Recommendations

A majority of security violations, vandalism, and even accidental acts that lead to disruption of services can be attributed to deficiencies in physical security. The guidelines below should be considered in order to maintain adequate physical security for the Palmyra Area School District.

Location

1) Locate computer equipment in inconspicuous places without signs, maps, and external references.
2) Locate network equipment away from windows or any other place that allows easy access by outside individuals.
3) Locate network equipment and computers in places that can be environmentally controlled.

Access

1) Rooms or closets that contain District Wide Area Network routers and servers must be locked at all times. This includes remote offices. The technology staff will be the only authorized party to enter these rooms.
2) Wiring closets should be locked at all times, with technology staff only authorized to enter the closets.
3) Switches are to be secured in a locked protected closet. While all switches are in rooms that can be locked, there are some switches in areas that are not in closets. The technology staff will be the only authorized party to enter these closets.
4) A secure access system should be installed and maintained in the main server room.
5) All users must log off the network (Novell) when they walk away form the computer. NO computer connected to the network should ever be left unattended by the user who logged into the network. All users must log off the network and shut down the computer at the end of the day.
6) All classrooms, offices and meeting rooms, etc. that house computers must be locked and secured when the room is vacated.

Environmental and Electrical Measures

1) Computer facilities must have fire protection. All facilities must have strategically placed hand held fire extinguishers. Fire extinguishers must be inspected yearly by the Fire Department.

2) All facilities must deploy smoke and heat detectors.
3) Flammable or toxic materials must not be stored near computer equipment.
4) Electrical systems for critical computer equipment must include Uninterrupted Power Systems(UPS). Surge protectors should be considered for equipment sensitive to power fluctuations.
5) Adequate room temperature and humidity must be maintained to the specifications of the hardware vendor.

Miscellaneous Physical Security Measures
Backup and recovery materials (tapes, manuals, etc.) should be kept at a site that meets stringent physical security measures.

Website; Privacy Statement, Disclaimer
The following is the Privacy Statement for PASD websites. This policy addresses collection, use, security of, and access to information that may be obtained through your use of the website. Users of said website understand and agree that in addition to this District Website Privacy Statement, each website you visit may have a unique Privacy Statement.

This notice covers the following topics:
The Palmyra Area School District has taken several steps to safeguard the integrity of its telecommunications and computing infrastructure, including but not limited to authentication, monitoring, auditing, and encryption. Security measures have been integrated into the design, implementation, and day-to-day practices of the entire portal operating environment. One of the key features is the use of SSL (Secure Socket Layer) for transmission of confidential information. This information should not be construed in any way as giving business, legal, or other advice, or warranting as fail proof, the security of information provided at www.pasd.us

Disclaimer
The PASD website could provide links to other web sites. These include links to web sites operated by other government agencies, nonprofit organizations, and private businesses. When a web user links to another site, the user is no longer on the PASD website and this Privacy Notice will not apply. When the web user links to another web site, the web user is subject to the privacy policy of that new site.

PASD Website Contact Information
To access your Personally Identifiable Information the District collects, if any, or to request correction of factual errors in the web user's Personally Identifiable Information or should the web user need further information on our Privacy Policy, the user should contact the Technology Supervisor.

Network Security Administration Procedures, Security Incident

Procedures, Reporting, Preserving Evidence, Legal Action

All security violations or suspected violations must be reported to the IT Services Department. The Department will then work with the principal or supervisor to ensure evidence is preserved and that it is reported correctly.

The Technology Department will then:

1) Respond quickly to ensure that traces, logs, etc. are intact and available. Processing will not be stopped immediately. No files will be restored immediately.
2) Communicate via the telephone. Some intruders may be able to monitor E-mail.
3) Make copies of files that the intruder may have altered of left.
4) Make sure the perpetrator is not directly contacted.
5) Identify a primary contact to handle evidence.
6) Contact the FBI and local Law Enforcement.

It is the responsibility of all district employees and/or contractors to report suspected security violations as quickly as possible. Subsequent action, depending on the type of breach, can vary. Security breaches may be categorized as those pertaining to physical intrusions, electronic intrusions that include networks, servers, and workstations; incidents related to catastrophic disasters, and breaches as a result of deception and/or fraud. The ultimate goal, regardless of the category of incident, is the protection of district/state assets, containment of damage, and the restoration of service.

Network Security Administration Procedures

Normal logging processes should be enabled on all host and server systems.

Alarm and alert functions, as well as logging, of any firewalls and other network perimeter access control systems should be enabled.

Audit logs from the perimeter access control systems should be reviewed daily.

Audit logs for servers and hosts on the internal, protected network should be reviewed on a weekly basis.

Users should be trained to report any abnormalities in system performance to the Technology staff.

Users should notify the Technology Coordinator, Network Administrator and Superintendent of violations of the CIPA law. All users must abide by the CIPA as stated in the Acceptable Use Policy. Violations will be reported to the proper legal authorities. Everyone who knows of the violation must report it to proper enforcement authorities.

All trouble reports received by the Technology Department should be reviewed for symptoms that might indicate intrusive activity. Suspicious symptoms should be reported to the Network Administrator and Technology Coordinator.

Security Incident Reporting Directions

1) Keep a Written Log of pertinent information.
2) Notification of Incident: Inform the appropriate people. In the case of a criminal act, secure the computer and store it until the incident has been investigated and cleared.
3) Control of Information: Control all information. Release to Superintendent.
4) Follow up Analysis. All involved parties should meet and discuss the actions.
5) Procedures should be evaluated and modified.

Physical intrusion of secured areas

1) Notify the Building Principal and Superintendent
2) If warranted, notify the appropriate authorities.

Catastrophic Disasters of secured areas

1) Notify the Building Principal and Superintendent
2) If warranted, notify the appropriate authorities.

Electronic Intrusions

1) Notify the Technology Supervisor, Technology Specialist, and Superintendent of schools.
2) Any data captured that resulted in detecting the intrusion should be kept until the incident has been investigated and cleared.

Deception and Fraud

1) Notify the Superintendent.
2) If warranted, notify the appropriate authorities.

Hacking Incidents

Attempts to Gain Access to a System: Incidents of this type may include repeated login attempts, repeated ftp or telnet commands, and repeated dial back attempts.

1) Identify the problem.
2) Identify the source
   a) look at system log files and
   b) active network connections
3) Make copies of all audit trail information:
   a) system log files,
   b) the root history file,
   c) utmp and wtmp files, etc.
4) Log all actions.
5) Notification
   a) Notify the Technology Coordinator, Network Administrator, and Superintendent.
   b) If warranted, notify the Department of Finance and Administration

Law Enforcement, and/or local police department.

6) Complete follow-up report.

Active Hacker/Cracker Methods for incidents

The method used to handle a cracker/hacker incident should be determined by the level of understanding of the risks involved.

Method 1. Immediately lock the person out of the system and restore the system to a safe state.

Method 2. Allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to an identification and possible criminal conviction.

1) Notify the Superintendent.
2) If warranted, notify the Department of Finance and Administration Law Enforcement, and/or local police department.

Gathering Evidence of Hacker/Cracker Incidents

1) Removal of Hacker/Cracker
2) Make a Snapshot of the system
3) Make copies of system log files,
4) Make copies of the root history files, etc.
5) Make a listing of all active network connections.
6) Log all actions.

Lock Out the Hacker

1) Kill all active process for the hacker/cracker
2) Remove any files or programs that he/she may have left on the system
3) Change passwords for any accounts that were accessed by the hacker/cracker.
4) Log all actions.

Restore the System

1) Restore the system to a normal stage.
2) Restore any data or files that the hacker/cracker may have modified.
3) Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited.
4) Document all actions in a logbook.

Report the Incident

1) Notify the Superintendent.
2) If warranted, notify the Department of Finance and Administration Law Enforcement, and/or local police department.

Follow up

1) After the investigation, a short report describing the incident and actions that were taken should be documented and distributed to the appropriate personnel.

Monitoring of Hacker/Cracker Activity

1) Make a Snapshot of the system.
2) Make copies of system log files.
3) Make copies of the root history files, etc.
4) Make a listing of all active network connections.
5) Record Monitoring information in a written log.

Software Procedures

1) Software owned or licensed by the Palmyra Area School District may not be copied to alternate media, distributed by e-mail, transmitted electronically, or used in its original form on other than district owned computers without express permission from the Technology Department. In no case is the license agreement or copyright to be violated.
2) Software licensed to the Palmyra Area School District is to be used for its intended purpose according to the license agreement. Employees are responsible for using software in a manner consistent with the licensing agreements of the manufacturer. License agreements are maintained by the Technology Department.
3) All software installed on PASD computers must be owned by the PASD.
4) All software purchased by the Palmyra Area School District must be installed on District-owned equipment, and may not be taken offsite without permission from the technology department.
5) No district owned software may be installed on a computer not owned by the District unless the license agreement specifically allows it.
6) There must be a separate software license for each computer unless a site license is purchased. Users may not purchase one software program or CD and install it on additional computers, such as every computer in the room.

Hardware Procedures

1) All workstations, printers, add-in cards, memory modules, and other associated equipment are the property of the Palmyra Area School District and should not be used for purposes other than business. No changes, modifications, or additions, or equipment removals may be done without written notification to the Technology Department and fixed asset manager. No information systems equipment should be removed from the district, with the exception of documented approval for equipment to be used for daily offsite work by a named, specific staff member.
2) In the event equipment is to be off premises for some time, the employee responsible for the equipment must file a written hand receipt with the IT department.
3) All computer and network electronics connected to the PASD network must be owned by the PASD or IU13 and must be on the fixed asset inventory.
4) A standard platform is established for district computers and equipment.
5) Approved non-standard hardware is only to be used when the standard

hardware is unavailable.

6) All hardware purchased by the Palmyra Area School District must be installed on District-owned equipment.
7) In order for effective software and network functioning, modern up-to-date computers, servers, routers, switches, etc. must be provided by the District.

Mobile Devices (Smartphones and tablets)
The Palmyra Area School District will establish procedures which allow it to keep track of mobile devices used to access district information and the personnel who use them.

Users who have been assigned a mobile device, both for long and short durations, shall be responsible to promptly report lost or stolen devices. The loss or theft of a device must be reported to both IT Services and the employee's immediate supervisor as soon as the loss or theft is identified. IT Services, via administration, shall contact law enforcement and the district's insurance carrier when theft is suspected.

IT Services shall maintain record of all assigned devices. Devices which have been configured to access business information or electronic mail shall have the capability enabled to remotely erase and render the device unusable. If these devices support the feature, a pass code lock shall be enabled at all times and entered by the user for access. The pass code lock shall be active when the device is idle.

Practices for Network Use:

1) No materials are to be disseminated in any manner which are derogatory to any person or group, obscene, racist, sexist, harassing or offensive based on color, religion, creed, national origin, age or disability.
2) System identification codes and passwords are for the use of the specifically assigned user and are to be protected from abuse and/or use by unauthorized individuals.
3) All e-mail messages are automatically scanned for viruses using the virus detection software installed on all computer workstations. If you have made any configuration changes to your workstation, even with the approval of the Technology Department, it is your responsibility to ensure virus protection prior to opening/executing diskettes, e-mail attachments or executable e-mail messages.
4) Like all IU13/PASD information systems resources,Internet access and e-mail are for work-related use. Access and sites visited can and will be monitored at the specific individual level.
5) Employees may not use PASD/IU13 information systems resources for soliciting, personal financial gain, partisan political activities, or further disseminating junk e-mail such as chain letters.
6) Information contained on the district's network and workstations is strictly proprietary to the Palmyra Area School District or State of Pennsylvania. All data stored on PASD computers and/or servers are the

property of the Palmyra Area School District. Copying or disseminating any of this information for any purpose other than district business is strictly prohibited. Access to this information must be considered confidential.

7) Users are expected to report violations of this policy which the user observes to the technology coordinator, network administrator or supervisor or, in the event that the violation involves the supervisor, the Superintendent. Likewise, if you are a witness to a violation you are required to cooperate in any investigation of the violation. All incidents and actions should be documented.

Consequences:
Any user who knowingly and willingly violates this policy is subject to discipline up to and including termination from employment, or expulsion from school, depending on the severity of the specific offense(s).

Furthermore, in the event of an illegal activity, the user will also be reported to the appropriate law enforcement authority. If you have any questions regarding this policy or any situation not specifically addressed in this policy, see your supervisor or the PASD Superintendent of Schools.

Revision of Security Policy:
This policy is subject to revision. The district will adequately post revisions, but it is the user's responsibility to ensure that use of the computing and communication resources conforms