

Communication PRinciples for Principals

FEBRUARY 2013

SECURITY OF INFORMATION TECHNOLOGY (IT) RESOURCES

Increasing information security is both a necessary and achievable task. It is the prudent thing to do for organizations and the right thing to do for students, parents, staff, and military communities.

Introduction

Securing Information Technology (IT) resources is a constantly evolving area which has become an integral part of national security and the Department of Defense (DoD) mission. Daily threats against information management systems residing in the Global Information Grid (GIG) (which houses the DoD and DoDEA IT systems) are increasing and require more diligence in protecting those systems. As these threats become more prolific, the risk increases and has become intolerable. Because DoDEA is part of the larger DoD information network, we all must act to protect the sensitive information of our families and employees and to fully comply with DoD requirements.

The challenge for DoDEA is to achieve a balance between the needs of the classroom and the implementation of DoD and the United States Cyber Command (USCYBERCOM) mandates. USCYBERCOM directs the operations and defense of specified Department of Defense information networks and prepares, when directed, to conduct full spectrum military cyberspace operations.

USCYBERCOM recently issued a requirement to ensure that all DoD agencies are in compliance with specific IT security controls. Many of these controls will impact on our school operations.

This tip sheet will provide principals with information and talking points to help employees better understand the need for greater security measures, the immediate steps that must be taken to implement and ensure IT security, and ways that we will address solutions for the future.

Security of the Networks

The need for information assurance increases every day for the Department of Defense. To ensure a more secure GIG, DoD entities, including CYBERCOM, are collaborating with other federal and industry partners to improve information security for the DoD.

DoDEA HQ Communications Office

4800 Mark Center Drive
Suite 04F09-02
Alexandria, VA 22350

Frank O'Gara: (571)-372-0613
DSN: 372-0613
Frank.O'Gara@hq.dodea.edu

Elaine Kanellis: (571) 372-0614
DSN: 372-0614
Elaine.Kanellis@hq.dodea.edu

Visit the DoDEA website
more information.
<http://www.dodea.edu>



What are some of the 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 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.



IDEA

Although there appears to be more threats that come from outside of the organization, internal threats are far more likely to breach system security than external threats.

What is the urgency?

Last fall, a computer virus that caused a shutdown of some critical systems in one DoDEA Area operation; the unintentional release of personal student data; and recent updated orders from U.S. Cyber Command, all speak to the necessity of implementing long standing mandates on the use of unapproved storage in DoDEA.

Technology security planning is a risk management issue

Because information technology security planning is primarily a risk management issue, DoDEA has expects users to assist in the creating a shared and trusted environment, with particular attention to:

- » Common approaches to end-user authentication;
- » Consistent and adequate network, server, and data management; and
- » Appropriate uses of secure network connections.

What is the scope of our IT operation and worldwide network?

- » 98,000 users
 - » 88,000 computers
 - » 2,200+ servers
 - » 2,100 software applications
 - » Over 150 Bandwidth Circuits
 - » Nearly 200 Wireless Networks (School-Level)
 - » Over 200 Video Teleconference/Telepresence systems
 - » Over 4,000 networking components
 - » Over 170,000 help desk tickets a year
- All of which are subject to DoD and DoDEA requirements.



IDEA

Like people who lock their doors, schools have always been concerned about protecting their valued resources, including confidential information contained in student and staff records.

Purpose of our systems

The information systems and Internet access available through DoDEA are available to:

- » support learning
- » enhance instruction, and
- » support school system business practices.

What's at Stake?

- » Vital administrative information that DoDEA must use to operate efficiently and fulfill its mission effectively;
- » Confidential student and staff information that DoDEA must maintain and be accountable for under federal law; and
- » Our ability to operate safely and securely within the larger DoD network environment.

What immediate steps must DoDEA take with regard to security?

Beginning February 25th, unapproved Removable Storage devices will be banned on all DoDEA computers. Removable Storage includes: thumb drives, memory sticks, camera memory cards, external USB hard drives, MP3 players, camcorders and printer memory.

Removable Storage devices approved for use include: DoDEA-owned and encrypted (Federal Information Processing Standards (FIPS) 140-2 certified) thumb drives; CD/DVD burners; Drobo type Multi-TB Devices; imaging devices; and media players. All approved devices must be registered with the appropriate Information Technology office prior to use.



IDEA

Security is defined as the ability to protect the integrity, availability, and confidentiality of information held by DoDEA activities and to protect network 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 web-based applications and connectivity.

Authorized users of Removable Storage also must provide documentation of:

- Annual Information Assurance Awareness Training,
- Privacy Act and Safeguarding Personally Identifiable Information Training and,
- A DoDEA Computer and Internet Access Agreement.

Removable Storage devices that will not be approved for use include any personal device containing Removable Storage, DoDEA-owned unencrypted thumb drives, and most DoDEA-owned external hard drives.

Safe and authorized alternatives for using Removable Storage devices

The ban on unauthorized removable storage devices on DoDEA computers will have an impact on our user community. There are options that are safe and authorized alternatives to using removable storage devices. It's important to note that each of these options includes specificity with regards to the transfer of Personally Identifiable Information (PII).

Option #1 - The DoDEA Gaggle.net Digital Locker

AUTHORIZED FOR PII: NO

This remains the preferred method for student and teacher use in transferring files. This no-cost solution provides up to 7GB of online storage for each student that is easily accessed from any internet-connected computer. This solution also has the added benefit that files in the digital locker are scanned for viruses and other malware. This is supplemental to scans that already occur on DoDEA computers. Data transfer to and from the Gaggle.net Digital Locker is also protected using military-grade encryption and the files are stored in a secure repository.

Option #2 - Rewritable CDs and DVDs

AUTHORIZED FOR PII: NO

Rewritable CD's or DVD's – This method is primarily for employees without Gaggle.net access and is an option for students and teachers alike. This solution relies on the computer having a CD/DVD burner installed. While this is standard in most computers purchased in the last 6 years, some older computers may not support this option. A rewritable CD or DVD is suggested as they can be reused many times. While not as secure as the Gaggle.net Digital Locker it does offer benefits not available on USB thumb drives. The primary benefit is that applications are prevented from automatically starting on CD's and DVD's inserted into DoDEA computers.

Option #3 - DoDEA Encrypted Drives and DoDEA Cloud

AUTHORIZED FOR PII: YES

These methods are authorized for the transfer of files containing PII. The DoDEA File Cloud will provide internet accessible storage (similar to Dropbox/Google Drive) using systems maintained by DoDEA IT. This method should also be used when transferring files too large to send using encrypted email. The cloud solution will be available to all DoDEA employees and students by the end of the current school year. Encrypted USB drives, specifically, are limited to employee use only due to cost of the devices. A list of DoD-approved devices will be maintained by DoDEA IT and provided to all personnel. Once registered, approved encrypted USB drives will be usable on all DoDEA computers.

What role do employees and users play in maintaining a secure network?

The DoDEA network was established by DoD and DoDEA to provide a private network infrastructure for the DoDEA Pre-K12 educational community. Therefore, it is the sole privilege of each and every DoDEA employee to participate in the K12 network.

Critical information security strategies rely primarily upon appropriate conduct on the part of personnel, and secondarily on the use of technological solutions. Every employee has a responsibility to help create and maintain an environment for DoDEA to maintain system security, data integrity, and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data. All DoDEA employees are bound to adhere to the policies developed to protect the system.

- » Employees should read and comply with DoDEA policies and regulations regarding use of its information systems including:
- » DoDEA information systems are operated for support of the educational mission of the school system. The use of the DoDEA's network is a privilege, not a right. Users should not do, or attempt to do, anything that might disrupt the operation of the network or equipment, interfere with the learning of students, or impair the work of other DoDEA employees.
- » The DoDEA network is connected to the Internet, a connection of networks, which enables people to interact with millions of networks and computers. The principal or IT office representative determines who may have access to the DoDEA network, and he or she may restrict or terminate any user's access, without prior notice, if such action is deemed necessary to maintain computing availability, ensure appropriate use, or protect security.
- » DoDEA computers, systems, and network resources are the property of the DoD and may not be altered in any way, unless authorized by a school-based IT office representative, Educational Technologist (ET), or IT program manager.



IDEA

The DoDEA Network was established by DoD and DoDEA to provide a private network infrastructure for the DoDEA Pre-K12 educational community. Therefore, it is the sole privilege of each and every DoDEA employee to participate in the K12 network.

- » Software instructions and license agreement terms must be strictly followed. Duplicating copyrighted software, without fully complying with license agreement terms, is a serious federal offense and will not be tolerated. Having a copy of a piece of software does not constitute authorization for modifications or additional copies of the software to be made; most licenses prohibit such uses. Installing unlicensed software is not permitted. Users should not install any software on school system equipment unless authorized by an AT or ET.



IDEA

Successful information security policy requires the leadership, commitment, and active participation of school administrators.

Enlisting the cooperation and support of employees

Implementing these measures will be painful for some employees. It is important to help them understand the importance of protecting the DoDEA and DoD IT networks and that their support and actions will help ensure that computer networks are safe and dependable environments.

There is potential for impact on educational programs that have relied heavily on Removable Storage. One way DoDEA is lessening the impact of new IT operating requirements includes implementing a state-of-the-art secure cloud solution.

As with any new technology change, you may identify issues that were not envisioned at the outset. Please raise any issues and recommendations to your local IT office and district Educational Technologist.

Maintaining security is every employee's responsibility. It applies to all DoDEA offices and schools that operate, manage, or use network services or equipment to support critical DoDEA mission requirements, including the delivery of instruction.

Role of the Principal in safeguarding our technology

Successful information security policy requires the leadership, commitment, and active participation of school administrators. The responsibility for meeting the sometimes competing expectations of employees, students, and the requirements placed on us the DoD is inescapable for building level administrators. Like it or not, it comes with the job.

Acknowledgements

Grateful acknowledgment is given to the U.S. Department of Education (Institute of Education Sciences) and Fairfax County Public Schools for use of some of their information and tips in this publication.