Risk Management Guidelines	Number: 10 – 04 Date Issued: July 17, 2017
Subject: LAPTOP THEFT PREVENTION PLAN	Expires: Until Superceded

I. OVERVIEW

District strongly believes that providing students and faculty with an ample supply of computers and other technology tools is a critical piece of its educational program and overall mission.

Unfortunately, as school sites have increased their investment in laptops over the past several years, **district** campuses have universally experienced a growing number of computer thefts. The loss of laptops not only denies students and teachers of a critical learning tool, but also costs our campuses substantial dollars in replacement and insurance claims.

In order to mitigate the loss of computers across **district** campuses, we have created a **Laptop Theft Prevention Plan** program to support school sites in preventing computer theft from occurring and to aid in the recovery of laptops in the event that a theft should occur.

While the **Laptop Theft Prevention Plan** places additional responsibilities on teachers, administrators, and site-based tech staff, CRMA has attempted to craft a simple, straightforward set of policies and procedures that both recognizes the day-to-day challenges our teachers face in managing a classroom, supports the original intent of having wireless campuses where technology is readily accessible, and establishes a clear system of accountability.

To accomplish its goals, the **Laptop Theft Prevention Plan** takes a layered approach to protecting school computers and has three main components: Facilities, Technology, and Operations.

II. FACILITIES

A. Goal: To prevent large break-ins where a large number of laptops are stolen at any one time.

Unfortunately, given our funding environment, securing an entire school building is impossible. Securing all exterior doors would require an elaborate array of sensors and/or motion detectors that is simply cost prohibitive. However, we strongly suggest that each school site have a monitored security alarm system for its outside entry doors. Further, we can go a long way towards securing our laptops from a facilities perspective by establishing a dedicated Computer Storage Room at all school sites.

B. Computer Storage Room: Because all of our school sites have different physical plants and layouts, it is impossible for all Computer Storage Rooms to be uniformly located across the network. When choosing a Computer Storage Room site, schools should keep the following characteristics in mind. The Computer Storage Room should have a single door as the only means of access. It should not have a window. If possible, the Computer Storage Room should not be located on the first floor of the building and should not be used for anything other than computer storage.

C. Computer Storage Carts: Inside the Computer Storage Room, computers should be housed in 2-3 large Computer Storage Carts with each unit capable of storing and charging 20 to 30 computers at any given time. These carts have two levels of security. First, the doors to the Computer Storage Carts can be locked. Second, the Computer Storage Carts can and should be locked into a docking station that is secured to the wall. The Computer Storage Room and Computer Storage Carts cabinets, the room should have a fully monitored alarm system with both door contacts and motion detection in the room. The alarm system should have a loud noisemaker outside the room.

D. Keys and Limiting Access: The door to the Computer Storage Room itself will have an additional lock and key. The lock should be different from all other locks in the building and key access to the Computer Storage Room should be limited to no more than the *Principal, School Operations Manager* and *Technology Coordinator*.

E. Nightly Storage: Because the Computer Storage Room and Computer Storage Carts units provide maximum security, it is advisable that the majority of all computers be returned to the Computer Storage Room at the end of every school day for nightly storage. However, because we realize that storing all computers in a single location is neither feasible not even advisable, we will discuss classroom storage in the Operations documents section of this document.

F. Summary: From a facilities perspective, the primary goal is to prevent a large number of laptops from being stolen all at once. This can best be accomplished by alarming the main entry points to your building, providing enhanced security to a single Computer Storage Room within your building, creating several physical layers or security within the Computer Storage Room, limiting access to the Computer Storage Room, and ensuring that the majority of your technology is returned to the Computer Storage Room on a nightly basis.

III. Technology

A. **Goal:** To signal to students and staff that laptops are able to be tracked, disabled, and recovered when and if they are removed from campus.

From a technology standpoint this goal can be achieved by addressing three distinct areas: Physical Appearance, an Inventory and Tracking System, and Computer Configuration

.

B. Physical Appearance: Establish a program to put security plates, tattoos, and stickers on each computer. Each plate will have a unique number that will be used for the inventory tracking system. The plates, tattoos, and stickers are very hard to remove and discourage resale. Various vendors can be used, including *STOP*, a leading provider of technology theft prevention products, and *WeTip*, an information facilitation service, among others. You may also augment this with a stencil unique to each site. This will further make the computer less attractive on the black market.

One other option to consider is to paint each laptop a unique color such as a bright pink or neon green. This will also make each computer less easy to disguise if taken and may discourage theft.

C. Inventory and Tracking System: Key to tracking technology assets and success in keeping them will be an Inventory and Tracking System.

Create a database of all computers and add other technology as necessary. If possible, use an online database that can be accessed over the web by all sites. This database can be facilitated through gathering computer data by installing a software agent on each machine that will report key data to the centralized database. The technology personnel at each site can augment this data. The site personnel should complete monthly audits and report on status of all assets.

One option to accomplish this is to adopt *ITAM* from *SchoolDude*, the nation's number one provider of online tools designed exclusively for the unique needs of educational facility professionals. There are other vendors who can also provide this service, so be sure to do research to determine the option that will best fit your school.

D. Laptop Configuration: Configure computers such that unauthorized users cannot log into the machine or reinstall the operating system. As a fail-safe, if someone does get into the computer's system, software can be installed that will photograph them and report their location to a recovery company over the Internet.

As a first layer of protection, require the use of a login screen. No computers will have automatic login enabled that lets the user have immediate access to the operating system. The login screen will also have a security warning. Require strong passwords that are not easily guessable.

Lock the firmware. This will require a separate password to boot from a disk or USB drive so reinstalling an operating system will be nearly impossible. This may be done on iMac's with Apple's Open Firmware Utility that is available for free. Other options for PC's are available as well.

Finally, consider installing *Orbicule's Undercover*. This software reports the user's whereabouts, takes their picture, compiles screen shots, and eventually disables the computer. At $8 per computer, we feel this is a worthy investment.

IV. Operations

A. Goal: To prevent the theft of individual laptops from classrooms and to create a clear system of accountability for laptops at the teacher and student level.

While the largest thefts occur after hours, computers consistently disappear in small quantities from classrooms over the course of the school day. These thefts seem to happen during instructional time and as students transition from one class to another.

While preventing all such is impossible, providing clearer direction for students and teachers around laptop check-in/checkout procedures and better classroom storage units should dramatically decrease the likelihood of laptop theft occurring during the school day.

B. Computer Storage Carts: Just as every school should have a single Computer Storage Room furnished with several large Computer Storage Carts, every classroom and teacher should be furnished with a smaller Computer Storage Cart capable of storing up to 10 laptops at once. The classrooms' Computer Storage Cart will provide teachers a safe and easy place to safely store any school laptops that may be in use in their classrooms on a day-to-day basis. Keys to the locks on the laptop cart security chains are maintained by the IT Manager and the office manager, who distribute them to teachers as they sign them out and retrieve them once they are signed back in the same day.

C. Individual Locks: In addition to having one Computer Storage Cart in every classroom, each teacher will be issued an individual lock for his/her own computer. These locks can and should be used to secure teacher laptops during the day and can easily be secured to large immoveable items such as a teacher's desk.

D. Keys and Locking Procedure: All school laptops should be stored in the classroom Computer Storage Cart at all times whenever a teacher is not physically present in the room. If a teacher requires that laptops remain in their classroom between periods or overnight, they should make sure that the laptops are locked in the classroom Computer Storage Cart before leaving their classroom. In addition, each classroom computer cart should have some means of being attached via docking mechanism or cable to the building or other large immovable item.

Each teacher will be issued a key to his/her personal Computer Storage Cart. No two classroom Computer Storage Carts in the school will work off the same key, thus holding each teacher accountable for all school laptops while in his/her possession. In case of the loss of a key, a master copy of all classroom Computer Storage Cart keys should be maintained by the Technology Coordinator only and stored safely in the school's Computer Storage Room.

E. Laptop Check-in/Checkout Policies and Procedures: While it is important for teachers to lock up equipment when they are not in the room, we recognize that laptop theft most often occurs during instructional time and transition time.

Based on staff feedback, laptops seem to disappear during these times due to the absence of a laptop check-in/checkout procedure that is simple, effective, and easy for teachers to implement. We believe that we have identified a set of policy and procedures that address these concerns.

F. Check-in/Checkout System: The lynchpin of the Tech Theft Prevention Plan during the school day is a very simple maxim. Teachers check out carts and students check out laptops. Conduct a weekly inventory of the mobile lab carts to ensure that all laptops and chargers are present. It is important to keep track of chargers, as the laptops are rendered useless without them and replacement costs are about $85 each.

Teachers check out Carts

Google Calendars for Staff: A Google calendar may be set up for cart checkouts. With each cart having a name, teachers will be able to reserve a cart for a particular period on a particular day. We recommend checking out the cart for large periods of time, for example, for half a day. We also do not think subsets of carts should be checked out by the teachers.

Students check out Computers

Student IDs for Students: Student IDs are increasingly being used across school sites for any number of purposes. In addition to current uses, student IDs can be used to effectively prevent laptop theft as well. Much like a library card that allows one to borrow books from the public library, student IDs can and should be used to check out and check-in laptops during the school day. Student level accountability can also include teachers keeping track of the ID number of the computer their students use, while a proxy server monitors in real-time, the internet sites accessed by each computer on the network.

When a teacher hands out a laptop to a student during class time, the teacher simply collects the student’s ID and stores them in safe but easily accessible place on his/her person. To retrieve his/her student ID, a student must return the laptop he/she was issued at the end of class.

Simple, effective, and easy to implement, this system creates accountability on both the part of students and staff and should prevent the majority of laptop theft during the school day.

For example, if a teacher hands a laptop to a student without requiring a student ID in exchange and the laptop goes missing during class, the teacher is accountable for the laptop’s loss. If a laptop disappears during class, the student whose ID is still in the teacher’s possession at the end of class is accountable for seeing that the laptop is returned.

G. Dos and Don’ts to Make the System Work:
Policies and procedures are only useful in so far as they are well implemented. Here are some basic dos and don’ts that should help ensure that the system as described above effectively combats laptop theft.

Don’t allow students to carry laptops from one classroom to another. If you do, the entire system breaks down.

Do require all students without exception to give you their student ID in exchange for checking out a laptop. Inevitably, some students will forget or misplace their student IDs over the course of the semester. However, as laptops are typically used for group work, this need not cause a breakdown in the system. If one student has forgotten or misplaced his/her student ID, simply ask another student in the group with an ID to assume responsibility for the group laptop.

Do not leave a classroom without locking all the laptops in the classroom in a secure area as detailed above. Any teacher who leaves computers in a classroom unsecured will be accountable for their return.

Do allow enough time at the end of class for students to return laptops. As simple as the new system is, it will still require a few additional minutes of time. Because student IDs are being used for a number of reasons at each school site, students will hopefully reinforce the new system by requesting their IDs back at the end of class.

H. Securing Laptops in Personal Vehicles: If there is a need for a staff member to take a laptop home, it should be properly secured in their vehicle. It should not be left out in plain view of any passersby and the vehicle should be properly locked. As with any other piece of equipment, the laptop should be treated as though it were the personal property of the staff member in that it should be secured properly so as not to invite theft. Also, time of year should always be taken into account and laptops should not be left in a hot vehicle in the summertime as it will cause all kinds of electrical problems.