Part A: Physical and Environmental Security

Answer the following based on the above given scenario.

Task A.1: Can physical and environmental security relate to cybersecurity? Explain and give reasons ? Yes, it can.

Explanation	Since 2016, there have been 855 cyber incidents publicly disclosed by U.S. schools and districts (K–12 Cybersecurity Resource Center). There were 348 in 2019 alone, almost triple the number in 2018. Security specialists are often so focused on technical sides that they miss out on the importance of physical and environmental controls but they are very significant in protecting and saving information. The expression of the physical and environmental security is measures taken to protect systems, buildings, and related supporting infrastructure against threats related to their physical and environmental surroundings. Physical security helps organizations secure assets, including IT infrastructure and servers, that make their businesses run and that store sensitive and critical data where Physical security encompasses measures and tools like gates, alarms, and video surveillance cameras, creating secure offices, rooms, and facilities, and implementing barriers to access, such as monitoring, and alerting, also includes another central element: an organization's personnel. For that, buildings that contain data and information technology systems must be granted proper protection to keep away from damage or unauthorized access to information and systems. Also, the equipment holding this information (e.g., data wiring, hard disks, laptop computers, and portable disk drives) must be protected, physically. Environmental security refers to the workplace environment. the workplace environment includes the design and construction of the facilities, how and where people move, where equipment is stored, how the equipment is secured, and protection from natural and man-made disasters. So, other issues should be considered, such as damage or loss caused by flood, fire, and sensitivity to temperature extremes. The NIST Cybersecurity Framework dividing physical security into three components: 1- Managing and protecting physical access to assets are mandatory. 2-Meeting policy and regulations regarding the physical operating environment for organizational assets is a must be. 3- Monitoring the physical environment to detect possible cybersecurity events. The technological development of the buildings and Security and Safety Systems have helped raise concerns about damage and increase the need for cybersecurity, it's important that security procedures keep up with the technological changes. Social Media: employees oversharing has allowed criminals to craft effective spear-phishing emails used to deceive employees into taking actions that sap security systems. This may lead to both digital penetration (data breaches and hacking) and physical penetration (robberies).
Reason 1	The physical environment needs to be monitored to detect potential cybersecurity events. Because physical access is the most direct path to malicious activity, including unauthorized access, theft, damage, and destruction. Therefore, buildings and rooms that house information and information technology systems must be afforded appropriate protection, including IT infrastructure and servers, that make their businesses run and

	that store sensitive and critical data. Besides, the equipment housing this information must be physically protected, and other issues should be considered, such as damage or loss caused by environmental conditions such as fire, flood, and sensitivity to temperature extremes.
Reason 2	Physical and environmental is related to cybersecurity because many offices and buildings become smarter and more digitized, they are secured with physical access control systems that utilize smart cards for identification. By holding a card near a reader authorized individual can enter a building or specific section within a building. Many of these systems, however, are connected to the Internet – raising possibilities that hackers could potentially allow unauthorized parties to gain access into a building, or into a sensitive region within a facility.

Task A.2: Identify potential threats and corresponding risks associated with physical and environmental security, and categorize them based on their impact on a particular perimeter and place (i.e., lobby, admin building, classroom, parking, and so on).

Threat	**Risks associated with physical and environmental security**	**Impact on**	**Perimeter Outer/Inner /Interior**
Theft **Threat type:** Physical security.	Loss of the availability of the instrument or lab/classroom equipment of the school. And the loss of the confidentiality of printed critical/sensitive information or stored in computers or servers due to the failure of a person to lock the gate or lack of physical security.	Admin building(room 123, 125, and 132), entry/exists gates and fence, stakeholders.	Outer/Inner /Interior
Fire **Threat type:** Environmental security.	Loss of the availability of Critical/sensitive information stored on computers or servers due to lack of the fire detection and alarm system.	Lobby, admin building, classroom, parking, stakeholder of the school, internal communications damaged, and external connectivity severed.	Outer/Inner/Interior
Accidental destruction **Threat type:** Physical security.	Loss of the availability of Critical/sensitive information due to allowing the staff to enter food/drinks to the sensitive area which may lead to spilling drinks on devices and causing damage or using infected USB, leave sensitive/critical information on the desk.	Admin building (Room 123, 125, and 132)	Interior
Power failures **Threat type:** Physical security.	Loss of availability of important/sensitive information stored on computers or servers due to the lack of an additional generator.	devices computer & servers & WIFI network, security cameras.	Outer/Inner/Interior

	Electricity fails or works incorrectly. Electricity pressure affects the electricity consumption, thus causing an increase in pressure on the devices, which leads to damage and disruption of the devices. Delayed in response to accidents, the electrical failure remains for a longer period.		
Damage that results from natural disasters(flood) **Threat type:** Environmental security.	Loss of the availability of Critical/sensitive information stored on computers or servers due to flood destruction.	Admin building (Room 123, 125, and 132), classrooms	Interior/Oute r

Task A.3: For each risk identified in the previous task, suggest a control strategy for each.

Risk	Control Strategy
Loss of the availability of the instrument or lab/classroom equipment of the school. And the loss of the confidentiality of printed critical/sensitive information or stored in computers or servers due to the failure of a person to lock the gate or lack of physical security.	1-Install turnstile doors in the visitor/staff entries to ensure sequencing entrance. 2-Use an access control system to allow only authorized personnel to enter the school (Id card). 3-The main door must be monitored and controlled by personnel that can turn people away when needed. 4-All visitors must provide identification in order to provide them with an access visitor card. 5-Assign security personnel (security guards) to assist the use of the access control system and help the visitor to provide them with visitor cards. And security personnel (security guards) rotation schedule must be defined. 6-Implement a surveillance system that must be monitored by the physical security team. 7-Unbreakable windows, full-height fence and exterior lights. 8-Multi-factor authentication should be used to access the computer labs(Room 123), classroom(Room 125) and sensitive facilities (Room 132). (password and fingerprint). 9-Encrypt the critical/sensitive information stored in the servers or computers. 10-Use secure cabinet to store printed critical/sensitive information that uses multiple opening mechanisms. (Key and code number) 11-secure disposal of the printed sensitive/confidential documents via shredder and using special devices to secure destruction of the school's critical assets. 12-Raise stakeholder awareness to report any suspicious behavior detected

	13-Incase if the theft detected incident response plan must be in place to know to deal with this threat
Loss of the availability of Critical/sensitive information due to allowing the staff to enter food/drinks to the sensitive area which may lead to spilling drinks on devices and causing damage or using infected USB, leave sensitive/critical information on the desk..	1-Increase employees' awareness of turning off their screens when devices are left unattended. 2-Need to set an automatic screen lock. 3-Use a privacy screen protector. 4-Not leaving documents on offices without supervision, specially protected and confidential documents. 5-Print protected and confidential documents on administrative printers in room 123 and requesting a code to enter. 6-During non-business hours the documents should be stored in a safe place. 7-Putting digital media such as USB and DVD should be in protected places to avoid unauthorized theft. 8-Ensure there are anti-virus programs on the computer and prevent students from using the USB stick. 9-Not to bring drinks and food into the devices rooms and be satisfied with that in the lunch break.
Loss of the availability of Critical/sensitive information stored on computers or servers due to lack of the fire detection and alarm system.	1-prevent the fire (Passive fire protection) by exterior walls, floors, and ceilings can be designed fire-resistant that, restricted vent access, fireproof. 2-Walls and Doors: The typical compartmentation system uses fire-rated walls and associated fire doors to contain the fire. 3-Use electrical equipment correctly like don't leave the wires exposed. 4-Perform a risk assessment in the cafeteria or kitchen on a regular automatic fire suppression system in case flammable liquids or cooking oils ignite. 5- (Active Fire Protection) intended to extinguish or control the fire-by-Fire detection is recognizing that there is a fire. Fire detection devices can be smoke-activated, heat-activated, or flame-activated. both manual and automatic, to perform their intended function, as well as notification to emergency personnel responding to the alarm. 6-fire dampers, Intumescent fireproofing is a layer of paint that is applied along with the coating system on the structural steel members, Intumescent coatings are applied as an intermediate coat in a coating system 7-Educating and preparing students for a fire emergency regular drills so that everyone is aware of their roles and the evacuation procedure plan building and office evacuation routes, choose and use fire extinguishers. 8-stations and sprinklers Safety recommendations include a certain number of proper sprinklers, fire alarm pulls, smoke detectors, and fire extinguishers within the building. 9-Ensuring that all fire alarms, sprinklers, and fire exits are in working condition is important.

	10-Periodic maintenance and pressure checks are essential for any fire extinguishing system to ensure it remains ‘fit for purpose.
Loss of availability of important/sensitive information stored on computers or servers due to the lack of an additional generator. Electricity fails or works incorrectly. Electricity pressure affects the electricity consumption, thus causing an increase in pressure on the devices, which leads to damage and disruption of the devices. Delayed in response to accidents, the electrical failure remains for a longer period.	1-Contracting with a team specialized in responding to emergency incidents 2-There is continuous periodic maintenance of electrical equipment. 3-Electrical Malfunction Control Squad. 4-The use of the electricity meter monitoring system and the alert is made when an error occurs. 5-Use of electricity pressure balancing system. 6-Contracting with a team specialized in responding to emergency incidents. 7-The presence of an additional generator in the event of a power outage. 8-The presence of an additional generator in the event of a breakdown of electricity at night to maintain the security of buildings, school fences, and cameras.
Loss of the availability of Critical/sensitive information stored on computers or servers due to flood destruction	1-Backup data to the cloud for sensitive data. 2-Placing servers and devices in protected rooms and placing them in the highest role. 3-Using the Flood Sensor in server and device rooms, this sensor triggers an alert when activated by water. 4-Using a Flood Berms and placing it near servers and devices in order to absorb water and form a protective barrier to prevent water from reaching the servers and devices. 5-Using Flood Barriers Mats and placing them on the floor of the servers and devices rooms, absorbing a 1 L of water and also wrapping it on the pipes that may leak water over the servers. 6-Ensure that the manufacture of doors and fences is of a strong type to confront the flood and prevent it from entering the school buildings. 7-Raise electrical sockets and wires to less than 1.5 meters above the ground.

Task A.4: Design policies to ensure physical and environmental security. The policies should be categorized using “Three Perimeters Strategy”. The policy document should cover all policy components as mentioned in W1S2 Slide#28.

Physical and Environmental Security Policies

OUTLINE:

1. Version Control

Policy Review This policy will be reviewed annually, or as new knowledge on the subject evolves and subsequent guidance is issued.

V.	Editor	Purpose	Change Description	Authorized By	Effective Date
1.0	EMCS Instruction	-	Original	School Administration	9/3/2021
2.0	M. Ghamdi	Guideline addition	Devices (servers, computer, printers and projector)	School Administration	19/3/2021

2. Introduction

[Objective 1: Provide context and meaning]

The schools were and still contain a lot of data for the school's employees and students. In light of the current situation and the accelerating changes, as well as the occurrence of natural disasters and the factors that affect schools, Schools are targets because of the sensitive data contained in IT systems, the need and focus on having a way to manage risks has doubled in the recent period by complying with the policy, which is the duty of all school's stakeholders. Because the school is keen to preserve its capabilities of human, financial, material and informational cadres

[Objective 2: Convey the importance of understanding and adhering to the policy]

the school has set up a policy aimed at identifying and predicting the risks that are expected to occur, reducing losses - if they happen - and mitigating their effects and creating a safe environment for all its material and informational components. These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this Policy,are implemented to reduce risks, and also protect resources from accidental or malicious damage.

[Objective 3: Acquaint the reader with the document and its contents]

A cybersecurity policy was created to be submitted and saved in the school, explaining the policies and controls used. A hard copy was placed inside the school, and the document was also uploaded to our school's website for viewing. Three of the school's policies are illustrated in terms of outer, inner, and interior involving physical and environmental security linked to cybersecurity. Outer policy, which includes protecting external doors and fences, and ensuring that they deter attackers. Inner policy It is responsible for the internal environment of the school in terms of ensuring the identity of staff, students, workers and visitors. Ensure that doors and windows inside buildings are protected. Also, make sure of the alarms, whether for fire or floods. Interior policy is responsible for the private offices and rooms that include the data of the school's stakeholders. During this policy, it was clarified the way in which all documents are protected, whether inside offices or documents in equipment such as devices, servers, printers and projector. We clarified some of the roles and responsibilities of the school, including security guards, from their duties to demonstrate the intent of the Outer Perimeter Security Policy and violations referred to the appropriate Board of Directors and management team. The Facilities Management Officer is responsible for accompanying the visitors during the school day and not leaving them unaccompanied until the end of the school day. The Compliance Officer is responsible for verifying the implementation of these policies, which have been established by the school administration.

[Objective 4: Explain the consequence of noncompliance as well as the exception process]

We will find some exceptions in these policies that concern the school's stakeholders. These exceptions are made because there are some situations in which implementation of the policy is not possible or there may be harm. These exceptions have been agreed upon by the school administration. This policy has been developed for full enforcement , and the school's employees will be trained on it. In the event of non-enforcement with this policy, disciplinary measures will be taken which may include dismissal for a period of time for students, termination of service for staff or legal accountability for school stakeholders. Compliance with this policy will be verified periodically by the school administration.

[Objective 5: Thank the reader and provide a seal of authority]

In conclusion, thank you for your support and your full commitment to these policies because we all strive to create a safe environment for all.

- The School administration

3. Outer Perimeter Security Policy

3.1 Policy heading

Overview

The school is responsible for keeping safe from harm, so the first layer of protection is The Outer Perimeter securing the perimeter during the school day but also during non-school hours This layer of security consists of solid walls or fencing and clear signage and locking devices on the perimeter gates that deter attackers and delays serious ones, which is the responsibility of the Board of Directors and management team, and security guards. because this doesn't enough to protestation the principal objective of a school's to the knowledge of control strategy for risk management.

3.2 Policy goals and objectives

1-To detection systems that make it more likely that the attack will be noticed, and a response capability to repel or catch attackers.

2-To demonstrate the intent of the Outer Perimeter Security Policy.

3-To define security guards roles and responsibilities.

4-To meet Safety outer perimeter.

3.3 Policy Statement

1-School must have different entrance points for vehicles(parking entry) and pedestrians (main entry)with one main entrance and exit for each ensuring safety for anyone entering the site that.

2-Must be used automatic iron doors allow only main entry the building that closes automatically after use, access control system restricts entry to authorized personnel only.

3-Must be in the entry utilizing smart cards for identification. By holding a card near a read security guard authorized individual can enter a building.

4-To ensure the long-lasting security and durability of schools must perform regular maintenance, checking hardware integrity and testing the functionality and security of gates, by the physical security team.

5-Must Security Cameras and prominently placed Install video surveillance systems, Set up video cameras in school parking lots and outside the building Use image or motion sensors near doors to monitor the movement, can record the suspicious activity then When a sound is detected, the device opens up a microphone so that security personnel of examination.

6-Must be Continuous remote surveillance allows authorized employees to monitor critical areas continuously, 24/7 in time are responsible by security guards.

7-The Night Vision Cameras transform average outdoor security systems are powered by infrared LED technology.

8-Must be Outdoor Lights integrate seamlessly with outdoor security camera systems. The moment they detect motion.

3.4 Policy exceptions

If there is a need for an exception to any outer perimeter security policy and/or procedures, for example, the main entry door should be closed after the non-work hours and can allow the parking door to open only. Alleged violations will be referred to the appropriate the Board of Directors and management team.

3.5 Policy enforcement clause

Should be the security of law enforcement investigative tools for criminal activity including theft and Cameras Aid Law Enforcement of law enforcement best investigative tools for school-related criminal activity including theft and vandalism.

4. Inner Perimeter Security Policy

4.1 Policy heading

The Inner perimeter of the building consists of doors, windows, and walls. The aim of this policy is to provide a framework for identifying and dealing with security risks facing the school, its staff, students, and visitors and Inner perimeter procedures delineate and maintain inner perimeters. This policy will allow the school, in as far as is reasonably practicable, to ensure the safety and security of the site and the people using these facilities from unauthorized entry. This physical security policy will ensure securing the protection of the second line of defense after the possibility of the attack crossing the outer perimeter.

4.2 Policy goals and objectives

1-To protect buildings and equipment from unauthorized access, misuse, damage, or theft.

2-Perimeter controls are required to protect equipment and building from environmental damage to facilities.

3-Maintaining measures that ensure that those in the school, including staff, students, and outside such as visitors and maintenance laborers, can perform their work in a safe and secure environment.

4.3 Policy Statement

1-Surveillance systems are a useful tool to control the flow of traffic into the inner perimeter so detection systems must include cameras, alarms, motion sensors.

2-Response systems should include locking doors, on-site or remote security personnel notification, and direct communication.

3-Must the typical compartmentation system uses fire-rated walls and associated fire doors to contain the fire and must Install turnstile doors in the visitor/staff entries to ensure sequencing entrance.

4- Ensure that the manufacture of doors is of a strong type to confront the flood and block it from entering the school buildings.

5-Exterior walls, floors, and ceilings must be designed as fire-resistant.

6-Ceilings must be waterproof.

7-Windows must be of a strong type of glass and iron windows.

8-Entrances must be illuminated because the lighting is a deterrent.

9-The presence of an additional generator if there is a breakdown of electricity at night to maintain the security of buildings, and cameras.

10-The use of the electricity meter monitoring system and the alert is made when an error occurs.

11-Ensuring that all fire alarms, sprinklers, and fire exits are in working condition is mandatory.

12-hiring a team specialized in responding to emergency incidents.

13-Periodic maintenance and pressure checks are important for any fire extinguishing system to ensure it remains fit for its purpose.

14-The biggest challenge is authorized entry; therefore, the staff and visitor must have identity cards.

15-Must use an access control system to allow only authorized personnel to enter the school (Id card).

16-All visitors to the school head office have to report to reception and sign in, to receive a badge before the entrance to the school. Visitors must be admitted to school premises only for specific authorized purposes.

17-Authorization and identification are required for entry to all nonpublic school locations.

18-Must assign security personnel (security guards) to assist the use of the access control system and help the visitor to provide them with visitor cards. And security personnel (security guards) rotation schedule must be defined.

19-For meetings involving external visitors held outside of public opening hours you will need to make arrangements for your visitors to gain access to the building. It is the staff's responsibility to ensure visitors are met and escorted to the meeting place and shown out of the building once the meeting has finished.

20-Must send emails before the meeting so that arrangements can be made with the on-duty caretaker for locking up the building.

21-Inner perimeter exit control via decontamination of outgoing personnel by using the security gate to detect metals .

22-If maintenance laborers are required to work outside of normal office hours, must follow the out of hours procedures.

23-Visitors are to be accompanied at all times and a record of visitors is kept in the security personnel (security guards).

24-Create a secure building culture and good security awareness campaigns and training programs.

25-All staff, contractors and visitors must display an ID card and wear it as an identification that can be evaluated remotely.

4.4 Policy exceptions

In the event of a possibility of fire, we will exclude point No. 21 from the internal perimeter policy, which is to control the exit from the inner surroundings by cleansing departing individuals.

4.5 Policy enforcement clause

1-The internal audit shall undertake independent reviews to assess the sufficiency of implemented security measures including compliance with the policy.

2-Security is everyone’s responsibility and all employees must make every single effort to respond to this Policy.

3-Staff must report suspected breaches of the policy immediately to the Practice Manager, if any suspicious individual in scope is found to have breached this policy one of the following consequences may be followed:

-Termination for employees and temporaries.

-Violation of contract and termination of employment relations.

- Individuals are subject to civil and criminal prosecution. To understand the implications of this policy or how it may apply to you, seek advice from your line manager and the board of directors, and the management team.

5. Interior Perimeter Security Policy

5.1 Policy heading

Overview

As a continuous effort to protect the interior of the buildings, office, labs, classrooms and sensitive/critical information, this policy developed. And this policy addressing the role and responsibilities of individuals to protect the school's valuable assets and high-level statements that must comply with to ensure our interior area is protected.

5.2 Policy goals and objectives

1-To protect our sensitive assets or information.

2-To define roles and responsibilities for the different stakeholders.

3-To meet applicable international requirements.

5.3 Policy Statement

General policies for offices, rooms, and facilities:

1-Staff must comply with a clear desk and clear screen policy. And the management must raise their staff's awareness about the general information security topics.

2-Areas that contain sensitive/critical assets or information must be classified as restricted areas.

3-Access to the restricted area must be based on a need-to-know basis, and the access list must be reviewed regularly.

4-Provided access must be updated when staff is transfer and revoked when it's left the school.

5-All surveillance system records must be regularly reviewed and kept for a minimum of 12 months.

6-The physical security team must monitor all the cameras of the surveillance system.

7-The facility management officer is responsible to maintain and test the Fair detection sensor in all school areas.

8-The facility management officer is responsible develop and maintain the surveillance system in all school areas.

9-Storage facilities must be secure and protected from unauthorized access.

10-All sensitive/critical information stored in computers or servers must be encrypted. And the list of the decryption keys must be stored in alternative sites.

11-Printed sensitive/critical information or removable media must be stored in a secure cabinet that has multiple opening mechanisms. And the removable media must be tested before being connected to the school's devices.

12-The incident response plan must be tested and documented.

Policies to secure Room 123, 125, and 132:

1-Staff must not enter any foods and drinks inside the labs, classrooms, or Admin building.

2-Visitors must not be allowed to enter the restricted area unless management approval is obtained.

3-The facility management officer is responsible for implementing a multi-factor authentication mechanism to access the computer labs, classroom, and sensitive facilities, (password and fingerprint).

4-Privacy screen protectors must be in place to protect the admin devices.

5-The facility management officer is responsible for controlling and monitoring the temperature and humidity of the room where servers are located.

6-Strong types of doors and walls of these restricted areas must implement and not from glasses.

Policies for removal of the physical and data equipment:

1-All staff must follow the removal of any data storage equipment procedures and guidelines to remove any data equipment.

2-Sensitive/critical information must be shredded when no longer needed.

3-All data stored in the devices must be deleted before the destruction of the devices.

5.4 Policy exceptions

This policy does not apply to areas that do not contain any sensitive assets or information such as the cafeterias, bathrooms, and regular classes.

5.5 Policy enforcement clause

Any violation of this policy may lead to disciplinary action, which may include termination for staff that fails to maintain and monitor interior physical security. Also, fines the individuals that attempt to destroy the school's instrument or equipment. Finally, individuals are subject to civil and criminal prosecution.

6. Administrative notations

Related Information:

CPTED (crime prevention through environmental design)

ISO/IEC 27002:2013 and NIST Cybersecurity Framework

Contacts:

Phone : 012-345-6789

Email: school37@sch.edu.sa

7. Policy definitions

ID badge: a small piece of metal or plastic with words or a picture on it, that you carry with you or fasten to your clothing or something else, in order to show who you are, that you are a member of a group.

Decontamination: monitoring the exit of departing individuals.

Risk management: the practice of identifying potential risks in advance, analyzing themes and taking precautionary steps to reduce the risk.

Attack: the act of attacking with physical force a antagonistic action launched for purpose stolen something.

Infrared LED technology: is a solid state lighting device that emits light in the infrared range of the electromagnetic radiation; pictureless can act like a spot light while remaining invisible to the naked eye.

Task A.5: Write down the guidelines and procedures for removal of any data storage equipment.

A lot of sensitive and private information is recorded in schools and stored on paper, devices and removable media. This information is recorded and preserved by the administration. When this equipment becomes obsolete or is no longer needed, sensitive or private data must be effectively removed from the storage equipment or destroyed before disposal. We put some guidelines around how to remove data storage equipment. This is in order to completely get rid of the data inside this equipment and also the inability to refer to it in any way.

Guidelines for removal of any data storage equipment	
1.	Destroy paper with Cross-cut shredding technology that produces 1 x 5 mm particles, in order to ensure that they are not tampered with after destroying.
2.	When the need to recycle the media , one of these two methods is used: - Wiping It is the process of writing new data to the media so that any old stored data is replaced with new data. - Use the process of Degaussing, during which it destroys the media by exposing it to a magnetic object and resetting it to a state close to zero. But if the need is the total destruction of the media, use this method: The purpose of destroying is to make the media unreadable or usable. The destruction of the media is done by a trusted third party, provided that there is a certificate of destruction.
	When you need to recycle devices, there is a method, which is: - Refer to the device manufacturer and determine if it is possible to disinfect it, or use a Cryptographic Erase to ensure that data recovery is not enforceable. Office equipment may contain removable storage media that apply sterilization techniques to the storage media in this equipment. But if the need is the total destruction of the devices, use this method: - The purpose of destroying is to make the devices not usable. The destruction of the devices include shred, disintegrate, pulverize, or incinerate by burning the device in a licensed incinerator are done by a trusted third party, provided that there is a certificate of destruction.

Procedures for removal of any data storage equipment	
1.Secure deletion for operating system Highly sensitive data (HSD) should be deleted as soon as it is no longer needed using one of the appropriate safe methods described below or equivalent.	**Secure Delete for Macintosh** For Macintosh OS-X 10.10 and earlier computers, the Secure Delete feature is included in the operating system. To access this feature, go to Finder, and select "Secure Empty Trash ..." located directly below "Empty Trash ..." from the Finder menu, and click OK. Note: If there is nothing in the trash, the menu item will be grayed out. OS-X version 10.11 (El Capitan) and later releases no longer have the Safe Delete option because all modern Macintosh computers have a solid state drive (SSD), and overwriting and deleting SSDs has proven not to be completely secure. So, if this Macintosh computer is approved for HSD storage, then full disk encryption, called File Vault, must be used. Deleting the file will be safe afterward as the files are encrypted. **Secure Delete for Windows** Safe deletion / shredding software should be used to safely and irreversibly remove data. The Windows Recycle Bin does not safely delete it. ITS provides a usable secure deletion program, called Secure Deletion Shredder, that places a new icon on your desktop. Use this program to destroy files and folders immediately and permanently.

2. Hard drive for data storage media Examples of data storage media include computer hard drives, floppy disks, CDs, DVDs, data tapes, flash drives, and memory cards, surveillance logs, cameras, computers, and their accessories. Procedures and methods for removing data from annually redundant hard drive are applied to prevent access to personal information on school data storage media when disposing of this media. **Use these steps to learn the correct way on how to remove a hard drive:**	**Step 1 Back up your data.** Copy your information onto an external hard drive or use another form of backup like online backup prior to removing your current hard drive. If your hard drive has failed and your data has been lost, skip this step. **Step 2 Turn off your computer and unplug it from everything.** you are going to want to get inside the pc , and it will be tons easier if it doesn't hang abreast of wires or suddenly turn on and electrocute you. Unplug the power source, monitor and the other devices. **Step 3 Open the computer case.** Each computer model is manufactured differently. Opening your specific case may involve removing a side panel with a screwdriver or pushing a button to open the case during a clamshell fashion. The owner's manual that came together with your computer should detail the way during which the case is opened. **Step 4 Locate the hard drive inside the computer case.** Within the computer, the hard drive might be placed during a cage that's either fixed to the tower or removable, or it might be placed on a group of rails. The hard drive may be a rectangular metal box the dimensions and width of a little book.By convention, most computers locate the hard drive near the front of the case, near other drives (like your optical drive). If you look closely, your hard drive are going to be clearly labeled intrinsically - don't go pulling random stuff out of your computer if you are not sure what it is **Step 5 Determine how the hard drive is connected to the computer.** Now that you've got located the hard drive, you wish to work out the way to remove it. You will need a screwdriver to open the cage and handle the drive if the hard drive is during a fixed or removable cage .Newer, more modern cases will often be "tool-less", meaning that you simply just need to push an easy lever or switch to be ready to remove the hard drive. **Step 6 Take the hard drive from where it rested within the tower** Hard drives will often sit on a group of rails towards the front of the computer case. Using both hands, carefully slide it outward.Pull carefully - if you encounter any resistance, stop! Nothing during a computer case should require any substantial amount of force - if you're pulling or pushing hard, you're probably doing it wrong. The hard drive will have two or more cables connected thereto . If those are impeding on your ability to require out the hard drive, remove these cables first. **Step 7 Remove the IDE ribbon cable.** This is often a broad, thin, usually gray ribbon running from your motherboard (or disk controller if present) to your hard drive. The cable could also be connected to the hard drive with glue, but you ought to be ready to work it out of place without much hassle. Carefully remove the maximum amount of glue as you'll and work the plug back and forth gently to interrupt the glue. **Step 8 Remove the facility connector** . This may be a plastic, rectangular connector with one or two latches depending on the extent of power your computer's motherboard provides to the hard drive(This connector will usually be tons more snug than the IDE ribbon cable. confirm you're disengaging the latches on the plug and pull firmly on the connector. lookout to not bend any of the skinny metal pins inside the plug. **Step 9 Take the drive out of the case and put it into an anti-static bag.**

Reference:

[1] https://biztechmagazine.com/article/2016/10/why-physical-security-should-be-important-cybersecurity

***[2]** https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/physical-and-environmental-controls*

***[3]** BOOK , Developing Cybersecurity Programs and Policies.*

[4] <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

[*5]* https://www.wikihow.com/Remove-a-Hard-Drive