SUBJECT: CIVIC – EDUCATION **CLASS: PRIMARY 5**

SCHEME OF WORK **2ND TERM LESSON NOTE**

WEEK ONE TO WEEK TWELVE

SCHEME OF WORK

WEEKS	TOPICS	LEARNING OBJECTIVES: At the end of the lesson the students should be able to:
1	Revision	Revision of last term work / welcome test
2	Security management	Meaning , examples
3	Security management	Meaning and types of security management
4	Security management	State and explain importance of security management
5	Security management	Precautionary measures in security management, risk
6	Safety and security management	Meaning and differences of safety and security management
7	**MID TERM BREAK**	**Midterm- Test**
8	Managing security	Meaning and examples
9	Threats to security	Meaning and examples
10	Combating security	Examples of security threats (in Nigeria)
11	Revision	General revision
12-13	Examination	Examination

WEEK: 1 REVISION OF LAST TERM WELCOME TEST

Second Term Security Education E-Lesson Note

WEEK: 2 **DAY:** **SUBJECT:**

DATE: **TOPIC:**

SUBTOPIC: **PERIODS:** **DURATIONS:**

PERFORMANCE OBJECTIVES : By the end of the lesson, most of the pupils should have attained the following objectives –

1. Explain the concept of Security management.

2. State the examples of security management.

ENTRY BEHAVIOUR : The pupils

INSTRUCTIONAL MATERIALS: The teacher will teach the lesson with the aid of security officer on duty.

CONTENT: SECURITY MANAGEMENT

LESSON 1 – INTRODUCTION

Security is the state of being free from all dangers or harms at home, in the school or anywhere you are. That's, feeling safe at all time.

Insecurity is when you are not feeling safe or free from dangers.

MEANING OF SECURITY MANAGEMENT

Security management is the process of managing the existing safety of lives and properties at all time.

EXAMPLES OF SECURITY MANAGEMENT

1. Quality security personnel

2. Threat assessment

3. Security register

4. Timely security report

5. Regular security monitor

6. Regular security check

7. Enlightenment

8. Control activities

PRESENTATION

To deliver the lesson, the teacher adopts the following steps:

1. Revises the previous lesson based on the pupil's related knowledge or understanding.

2. Displays a chart showing CCTV camera, dog, security guard, etc.

3. Lets the pupils analyze the content of the chart.

4. Asks pupils, why people use some these things at home and business.

Pupil's Activities – State the reasons for using cctv camera, dogs and security guards at home and other places.

5. Uses the chart and the pupil's responses to introduce the lesson and leads a discussion on the meaning of security management with appropriate examples.

Pupil's Activities – Participate actively in the class discussion.

6. Summarizes the lesson on the board.

Pupil's Activities – Write as instructed.

CONCLUSION

To conclude the lesson for the week, the teacher revises the entire lesson and links it to the following week's lesson.

LESSON EVALUATION

Ask pupils to:

1. Explain the concept of security management.

2. Give appropriate examples of security management with their locality.

WEEK: 1 **DAY:** **SUBJECT:**

DATE: **TOPIC:**

SUBTOPIC: **PERIODS:** **DURATIONS:**

PERFORMANCE OBJECTIVES: By the end of the lesson, the pupils should be able to:

1. Define security management.

2. Explain types of security management.

Resources and materials: Scheme of work, Online information Instructional material: Picture chart

Second Term Security Education E-Lesson Note

Building Background/connection to prior knowledge: pupils are familiar with the topic from their previous classes.

CONTENT: TYPES OF SECURITY MANAGEMENT

MEANING OF SECURITY MANAGEMENT

Security management is the process of managing the existing safety of lives and properties at all time.

Types of Security Management

Security management can come in various different forms. Three common types of security management strategies include information, network, and cyber security management.

#1. Information Security Management

Information security management includes implementing security best practices and standards designed to mitigate threats to data like those found in the ISO/IEC 27000 family of standards. Information security management programs should ensure the confidentiality, integrity, and availability of data.

Many organizations have internal policies for managing access to data, but some industries have external standards and regulations as well. For example, healthcare organizations are governed by the Health Insurance Portability and Accessibility Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) protects payment card information.

#2. Network Security Management

Network security management is a vital component of a network management strategy. The network is the vector by which most cyberattacks reach an organization's systems and its first line of defense against cyber threats. Network security management includes deploying network monitoring and defense solutions, implementing network segmentation, and controlling access to the network and the devices connected to it.

#3. Cybersecurity Management

Cybersecurity management refers to a more general approach to protecting an organization and its IT assets against cyber threats. This form of security management includes protecting all aspects of an organization's IT infrastructure, including the network, cloud infrastructure, mobile devices, Internet of Things (IoT) devices, and applications and APIs.

Security Management Architecture

A scalable and sustainable security management strategy is one that is built using an integrated framework and the right tools rather than a disconnected set of standalone policies and strategies. A security management architecture enables an organization to consistently enforce its security policies across its entire IT ecosystem. This requires an array of integrated security solutions that enable centralized management and control of an organization's entire security infrastructure.

Impact of DevSecOps on Security Management

A shift is on to automate security management using DevOps. There are many security tasks that are repetitive and take time to complete when using a management user interface. Security automation is a valuable tool for reducing the time spent completing tasks.

Examples of security management tasks that could benefit from automation include:

- Adding rules and objects to a security policy to complete a new project.
- Responding to a security incident by validating threat indicators, mitigating the threat by isolating the infected host, and searching logs for other infected hosts using Indicators of Compromise (IoC) returned from the security incident analysis.
- Provisioning new cloud infrastructures, including the firewalls and the security policy for the firewalls protecting the new infrastructure.
- Cloud applications of DevSecOps include container image scanning, code scanning, Infrastructure as a Code (IaC) scanning, and scanning for credential exposure.

Security Management with Check Point

Effective security management requires having the right tools for the job. One critical tool for security management is a cybersecurity platform that enables an organization to maximize the effectiveness and efficiency of its security team. Without proper monitoring and management, even the best security solutions cannot protect an organization against cyber threats.

Security management has always been one of Check Point's core competencies, and we continually work to evolve security and management capabilities to meet the evolving needs of the market and our customers. Check Point security management can be deployed on the platform of your choice; turn-key security management appliances, open server hardware, in public and private cloud environments, and as a hosted cloud service. Check Point's security management solutions are based on four key pillars, including:

- **Security Automation into CI/CD Pipelines**: Integrating security into CI/CD pipelines via automation reduces configuration errors, makes rapid deployments possible, and allows operational processes to be orchestrated.
- **Security Consolidation**: Consolidated security improves efficiency, reduces capital and operational expenditure (CAPEX and OPEX), and achieves improved visibility and context by integrating security policy and events management within a single solution.
- **Solution Agility**: Security management solutions must be agile and dynamic to keep up with the evolving cyber threat landscape. An example is an object in the security policy that defines private or public cloud addresses or users. As these external entities change, so does the security policy.
- **Efficient Operations**: Security should be a business enabler, not a roadblock. Security management solutions must be efficient to not inhibit security innovation. For example, easy to use management that unifies security and event management and enables delegated access to multiple admins at the same time enables security staff to do more in less time.

Second Term Security Education E-Lesson Note

WEEK: 4 **DAY:** **SUBJECT:**

DATE: **TOPIC:**

SUBTOPIC: **PERIODS:** **DURATIONS:**

PERFORMANCE OBJECTIVES: By the end of the lesson, the pupils should be able to:

1. State the importance of security management.

2. Explain the importance of security management.

Resources and materials: Scheme of work, Online information, Instructional material: Picture chart

Building Background/connection to prior knowledge: pupils are familiar with the topic from their previous classes.

CONTENT: IMPORTANCE OF SECURITY MANAGEMENT

Purpose of Security Management

The goal of security management procedures is to provide a foundation for an organization's cybersecurity strategy. The information and procedures developed as part of security management processes will be used for data classification, risk management, and threat detection and response.

These procedures enable an organization to effectively identify potential threats to the organization's assets, classify and categorize assets based on their importance to the organization, and to rate vulnerabilities based on their probability of exploitation and the potential impact to the organization.

In every type of organization, security plays an important role. The organization have to keep an eye on his important data. The concept of security management revolves around the **protection** of company data from unauthorized people. Nowadays every individual or company make his data stored electronically. Whether its bank, online store, airline or any other company. An organization trains his employees about how to be secure from hackers. An important thing organization do is install anti-virus software on every computer and protect 3rd party access by computer firewall. A firewall protects user computer from access of unauthorized apps.

Overview of security management

One key point about security management in an operating system is that you have to update your operating system and all the apps used in the operating system. Also, you must have the latest version of the operating system. And there is some mechanism by which your daily data is backup on some server. The administrator of the company has to save all daily data in a safe server. Also, there should be multiple backups on different servers. Company manager has to enforce employees to follow certain rules of data protection to avoid the risk of data loss.

One important thing to note is that if an employee is fired from the company then the manager has to instantly remove that user account from company computers so that he cannot make any damage to the company. If you are communicating with customers and suppliers often in a day then you have to make privacy on that part also e.g. you don't have to give company private information to the customers and suppliers. Internal information is the assets of the company. The information should be categorized into different categories. Categories of information may be the public type which can be shared publically, also information may be confidential that is known to the owner and some high management of the company. And some information is private that is shared with the employees of the company.

Individuals have to also follow some security management rules e.g. if they are using smartphones or tablets then they have to also install anti-virus app on it. And individuals have to not install any 3rd party apps on their smartphones and tablets. If you are using an older version of the mobile operating system then it is time to update the operating system. In most of the areas, the internet is accessed through a wireless network. So you have to restrict wireless network with authentication and encryption so that unknown user cannot access the network.

In any type of small or big organization, CCTV cameras play an important role. You can monitor customers and employee's performance and check if any assets of the company are misusing. If a company manager notices any fault part in the organization then it should be removed or make offline so that it cannot be accessed by the customers.

New user accounts in the company have to be checked and that account has to be restricted from accessing important data of the organization. Also, it should be noticed whether that user account is to be given access to the internet or not. All the user accounts have to reset their password after some days. And if you are an administrator in the company then you have to not tell password of any user to any other person in the company. Finally, high-level management of the company has to make rules so that future security planning and risk management is handled accurately.

Home security is the precautions taken at home to ensure safety of our lives and properties.

HOME SECURITY TIPS

The following are the security tips at home,
1. Look the doors and windows properly.
2. Check all doors and windows if they are properly locked.
3. Turn off all unused electrical appliances.
4. Keep valuable materials properly.
5. Know your neighbours very well.
6. Install burglary.
7. Install security cameras.
8. Inform your trusted neighbours if you are traveling.
9. Educate your children on security tips.
10. Stay safe always.
11. Call for help during emergency, etc.

PERSONAL SECURITY TIPS IN THE SCHOOL AND ON THE ROADS
1. Know your parent's contact number.
2. Obey the school's safety rules.
3. Follow the teacher's safety instructions.
4. Go home straight after school.
5. Do not go home before closing time.
6. Play on the school's playground.
7. Know your parent's contact number.
8. Do not give strangers your parent's contact number, etc.

PERSONAL SECURITY TIPS ON THE ROAD
1. Do not answer strangers.
2. Do not accept gift from strangers.
3. Do not play on highway or busy roads.
4. Make use of pedestrian bridge to cross to other side of the road.

5. Make use of zebra crossing.
6. Always walk on the pavement or footpath if there is one.
7. Walk facing oncoming traffic.
8. Know your parent's contact number.
9. Do not give strangers your parent's contact number, etc.

SECURTIY IN THE SOCIETY

Societal security relates to: "**the ability of a society to persist in its essential character under changing conditions and possible or actual threats**." The Securitization Theory When it comes to researching the EU's securitization of the Belt and Road initiative, the acclaimed Copenhagen School provides some useful ...

WEEK: 5 **DAY:** **SUBJECT:**

DATE: **TOPIC:**

SUBTOPIC: **PERIODS:** **DURATIONS:**

PERFORMANCE OBJECTIVES: By the end of the lesson, the pupils should be able to:

1. **Define precautionary measures in security**
2. **State and explain the precautionary measures in security management**

Resources and materials: Scheme of work, Online information, Picture chart

Building Background/connection to prior knowledge: pupils are familiar with the topic from their previous classes.

CONTENT: PRECAUTIONARY MEASURES IN SECURITY MANAGEMENT

Precautionary measures on personal security means **things a person a can do to make sure that he/she is secure**. It also means what a person can do in advance to ensure personal safety or to prevent personal insecurity. Precautionary measures on personal security include the following. 1 – Being careful with strangers.

What are the precautionary measures necessary when performing tasks?
Personal protective equipment (PPE)

- Gloves.
- Eye protection/face protection.
- Hearing protection.
- Coats/aprons.

- Footwear.
- Head protection.
- Height safety equipment.

We usually don't think that something bad would happen to us every day we go to work for instance – as it would drive us mad – but some precautions don't hurt. Let's see 15 simple personal security tips to keep in mind every day.

1. **Always be engaged in situational awareness** – meaning to keep attention at everything around you, from cars, to buildings, to people.
2. **Don't walk with both earbuds in your ears listening to music** in the street – you should be attentive to cars and people and vigilant to anything approaching you.
3. **Walk with your head straight and look at people in the street and your surroundings** – you will be less likely taken by surprise.
4. **Keep your head up at all times and don't text while walking.** Also, limit your phone conversations while you are walking so you'd be less distracted.
5. **Avoid suspicious or dangerous areas at night** or at least have company while crossing such areas.
6. **Walk with your keys in your hand whenever you cross a suspicious area** / neighborhood during the night or day; the keys can be used, ultimately, as a self-defense mechanism.
7. **Keep your car doors locked in case you have a purse, briefcase or valuables placed on the passenger's seat**; in fact, it is better to drive with your doors locked even if you don't have anything of value in the car.
8. **Always keep your family and friends informed whenever you travel**; write them text messages, send photos or call them so they know you are alright at all times.
9. **Be aware of pickpockets in crowded buses or subways**; keep the bag as close to you as possible, fully closed and secured.
10. **Be aware of all the exit routes in your office, the cinema, the mall and all other places you frequent**; you may think that nothing can happen to you, but it's better to be alert and have in mind more than one way out in case of a fire or other danger.
11. **Don't walk in the elevator with another person if you don't feel comfortable with that person**, you can wait for the next elevator or take the stairs.
12. **Turn and go in an opposite direction or enter a store / retreat to a public place if a stranger in a car approaches you and offers to give you a ride somewhere.**
13. **Close and secure your front door and windows at night** even if you live in a safe neighborhood or a high floor flat – burglars are more creative than you imagine.
14. This goes without saying, but it's better to repeat it: **be very careful at the ATM**, don't approach the machine if you see people just hovering around the ATM and never count your money in public.
15. **Keep a Red Panic Button app at hand.** In case you get lost or you find yourself in a dangerous situation, a simple push of the Panic Button will send a discrete distress call to a pre-set list of emergency contacts together with your GPS location so your friends and family can find you fast and easy.

WEEK: 6 **DAY:** **SUBJECT:**

DATE: **TOPIC:**

SUBTOPIC: **PERIODS:** **DURATIONS:**

PERFORMANCE OBJECTIVES: By the end of the lesson, the pupils should be able to:

1. Define safety, security management.

2. Explain examples.

Resources and materials: Scheme of work, Online information, Instructional material: Picture chart

Building Background/connection to prior knowledge: pupils are familiar with the topic from their previous classes.

CONTENT: SAFETY AND SECURITY MANAGEMENT

MEANING OF SAFETY

Safety means keeping yourself and others free from harm or danger. That's being careful not to fall, bump or run into things.

SAFETY DEVICES

1. Fire extinguishers
2. Apron
3. Boots
4. Hand gloves
5. Eye shield or goggles
6. Caution signs
7. Seat belts
8. Road signs -zebra crossing
9. Face masks,
10. Dust masks
11. Hearing protection

Security is the state of being free from all dangers or harms at home, in the school or anywhere you are. That's, feeling safe at all time.

Second Term Security Education E-Lesson Note

Insecurity is when you are not feeling safe or free from dangers.

MEANING OF SECURITY MANAGEMENT

Security management is the process of managing the existing safety of lives and properties at all time.

EXAMPLES OF SECURITY MANAGEMENT

1. Quality security personnel
2. Threat assessment
3. Security register
4. Timely security report
5. Regular security monitor
6. Regular security check
7. Enlightenment
8. Control activities

WEEK: 7- MIDTERM BREAK MID-TERM TEST

WEEK: 8 DAY: SUBJECT:

DATE: TOPIC:

SUBTOPIC: PERIODS: DURATIONS:

PERFORMANCE OBJECTIVES: By the end of the lesson, the pupils should be able to:

1. Define managing security.

2. Explain types of risk security management.

Resources and materials: Scheme of work, Online information, Instructional material: Picture chart

Building Background/connection to prior knowledge: pupils are familiar with the topic from their previous classes.

CONTENT: MANAGING SECURITY

What is meant by managing security?

Second Term Security Education E-Lesson Note

Security management **covers all aspects of protecting an organization's assets – including computers, people, buildings, and other assets – against risk**.

How do you manage risk in security?

Given a specific risk, there are five strategies available to security decision makers to mitigate risk: **avoidance, reduction, spreading, transfer and acceptance**.

Risk options

Risk avoidance

The first choice to be considered is the possibility of eliminating the existence of criminal opportunity or avoiding the creation of such an opportunity. When additional considerations or factors are not created as a result of this action that would create a greater risk. For example, removing all the cash flow from a retail outlet would eliminate the opportunity for stealing the money, but it would also eliminate the ability to conduct business.

Risk reduction

When avoiding or eliminating the criminal opportunity conflicts with the ability to conduct business, the next step is reducing the opportunity of potential loss to the lowest level consistent with the function of the business. In the example above, the application of risk reduction might result in the business keeping only enough cash on hand for one day's operation.

Risk spreading

Assets that remain exposed after the application of reduction and avoidance are the subjects of risk spreading. This is the concept that limits loss or potential losses by exposing the perpetrator to the probability of detection and apprehension prior to the consummation of the crime through the application of perimeter lighting, barred windows, and intrusion detection systems. The idea is to reduce the time available for thieves to steal assets and escape without apprehension.

Risk transfer

The two primary methods of accomplishing risk transfer is to insure the assets or raise prices to cover the loss in the event of a criminal act. Generally speaking, when the first three steps have been properly applied, the cost of transferring risks is much lower.

Risk acceptance

All of the remaining risks must simply be assumed by the business as a part of doing business. Included with these accepted losses are deductibles, which have been made as part of the insurance coverage.

WEEK: 9 & 10 **DAY:** **SUBJECT:**

DATE: **TOPIC:**

SUBTOPIC: **PERIODS:** **DURATIONS:**

PERFORMANCE OBJECTIVES: By the end of the lesson, the pupils should be able to:

1. Define threat to security.

2. Explain examples of threat to security.

3. Explain type of security threat

4. Explain combating threat to security

Resources and materials: Scheme of work, Online information, Instructional material: Picture chart

Building Background/connection to prior knowledge: pupils are familiar with the topic from their previous classes.

CONTENT: THREATS TO SECURITY

It means A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

Cyber threats are sometimes incorrectly confused with vulnerabilities. Looking at the definitions, the keyword is “potential”. The threat is not a security problem that exists in an implementation or organization. Instead it is something that *can* violate the security. This can be compared to a vulnerability which is an actual weakness that can be exploited. The threat always exist, regardless of any countermeasures. However, countermeasures can be used to minimize the probability of it being realized.

Types of security threats

The NIST definition above states that a threat can be an event or a condition. An event, in this case, also includes natural disasters, fire, and power outage. It is a very general concept. In cybersecurity, it is more common to talk about threats such as viruses, trojan horses, denial of service attacks.

Phishing emails is a social engineering threat that can cause, e.g., loss of passwords, credit card numbers and other sensitive data. Threats to information assets can cause loss of confidentiality, integrity or availability of data. This is also known as the CIA triad.

The CIA triad, together with three other well known security concepts, is the basis for the STRIDE threat model. When listing possible threats, it is convenient to use an existing classification as a starting point. STRIDE is the most well-known classification, proposed by Microsoft in 1999. The name comes from the initial letters of the different categories, which also makes it easier to remember them.

Threat	**Meaning/Example**	**Related Security Property**
Spoofing identity	An example is to use someone else's password and authenticate as that person.	Authentication
Tampering with data	This includes e.g., modification of data. Either data at rest or data sent over a network.	Integrity
Repudiation	This means that users can deny having performed an action, e.g., sending or receiving data.	Non-repudiation
Information disclosure	This includes a user reading data without granted access, or eavesdropping a communication channel.	Confidentiality
Denial of service	This relates to the availability of a system	Availability
Elevation of privilege	In these types of threats, a less privileged user gets higher privileges. Normal users obtaining root privileges is the most typical and severe form of this	Authorization

Examples of security threats

Recall that a threat is very general. It does not include *how* to realize it, or even if it is possible in the current system. Here are a few examples.

- A malicious user reads the files of other users.
- An attacker redirects queries made to a web server to his own web server.
- An attacker modifies the database.
- A remote attacker runs commands on the server.

Each of these examples can easily be mapped to a category in STRIDE. Other examples would be malware, trojans and worms.

Related terminology

There are several other terms that are closely related, but that should not be confused by threat.

- **Threat actor or threat agent.** This is the entity that carries out and realizes the threat. This is often instead called attacker or adversary when it is carried out by a person or a group. In that case it is also a deliberate action.

- **Threat action.** This is the actual attack, or the realization of a threat. It can take advantage of a vulnerability, but in e.g., the case of natural disaster, it does not have to be an underlying vulnerability that causes the threat to be realized.
- **Threat consequence.** This is the actual result when the threat is realized. RFC 4949 lists four main categories of consequences, namely “unauthorized disclosure”, “deception”, “disruption”, and “usurpation”.

COMBATING SECURITY THREATS – IN NIGERIA

What are the 5 levels of threat?
There are 5 levels of threat:

- Low - an attack is highly unlikely.
- Moderate - an attack is possible but not likely.
- Substantial - an attack is likely.
- Severe - an attack is highly likely.
- Critical - an attack is highly likely in the near future.

What are the negative issues associated with terrorism in Nigeria?

Nigeria continues to face multiple challenges posed by various terrorist groups with **devastating human cost, in terms of lives lost or permanently altered, internally displaced persons and immensely negative consequences for economic and social development**.

What are the examples of insecurity in Nigeria?

Insecurity in Nigeria is a recurring phenomenon that threatens the well-being of its citizens. The south-west of Nigeria is plagued by a surge in **cybercrime, armed robbery, kidnapping, domestic crime, extrajudicial killings, herder-farmer conflicts, ritual killings, and banditry**.

WEEK: 11- REVISION

WEEK: 12- EXAMINATION

WEEK: 13- EXAMINATION