

**SCHEME OF WORK (CBET CLASSES)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **DEPARTMENT: ICT** | | | | **NAME OF TRAINER: DUNCAN NDEGWA** | | | **NUMBER OF TRAINEES: 15** | | |
| **UNIT CODE: IT/CU/ICT/CR/3/6** | | | | **TERM: I** | **DATE OF PREPARATION: 22/12/2024** | | **CLASS: DICT/S23/J24** | | |
| **COURSE:** | | | | | | | **LEVEL: LEVEL 6** | | |
| UNIT OF COMPETENCE:  ICT SECURITY THREATS | | | | | | | **DATE OF REVISION: 3/1/2025** | | |
| **SCHEDULE** | | | | | | | | | |
| **WEEK** | **NUMBER OF HOURS** | **ELEMENT / LEARNING OUTCOME** | **SUB -TOPIC/ CONTENT** | **SPECIFIC OBJECTIVES / PERFORMANCE CRITERIA** | | **ACTVITIES** | | **REFERENCE/ RESOURCES** | **REMARKS** |
|  | **REPORTING AND REGISTRATION** | | | | | | | | |
|  | 4 | Introduction to ICT security threats | * Definition of security threats | * Categories of security threats * Internal * external | | * Taking notes * Class discussion * Questions and answers | | * https://[www.coursehero.com/file/11659891/Employee-sabotage**/**](http://www.coursehero.com/file/11659891/Employee-sabotage/) * Cyber Security, authored by John G. Voeller published by Wiley 2014 |  |
|  | 4 | Importance of Computer Security to an Organization | * Importance of Computer Security to an Organization | * Understand the role of computer security in protecting organizational assets. | | * Taking notes * Class discussion * Questions and answers | | * . * Cyber Security, authored by John G. Voeller published by Wiley 2014 |  |
|  | 4 | Identify security threats | * Fraud and theft * Employee sabotage * Loss of physical and infrastructure support * Malicious hackers and code | * Security threats are identified based on the vulnerability of the system. * Security threats are categorized according to the risk impact | | * Taking notes * Class discussion * Questions and answers | | * Cyber Security, authored by John G. Voeller published by Wiley 2014 * : https://youtu.be/Ces7UeMQ7ic |  |
|  | 4 | Identify security threats | * Industrial espionage * Threats to personal privacy * Natural Calamities * Cyber crime | * Appropriate security measures are selected as per the security threats | | * Taking notes * Class discussion * Questions and answers | | * Cyber Security, authored by John G. Voeller published by Wiley 2014 |  |
|  | 4 | Establish and install security measures | * Definition of security risk management * Benefits of Risk management | * ICT Security policy is implemented as per the Kenya Security Act 2018 * Evaluation of Security control measures is done as per the ICT Security policy | | * Practical * Oral questioning * Written tests | | * Cyber Security, authored by John G. Voeller published by Wiley 2014 |  |
|  | 4 | Establish and install security measures | **Risk management procedures**   * Risk assessment * Risk mitigation Uncertainty analysis * interdependencies * cost considerations   Benefits of security measures | * Installation of Security control measures is done as per the ICT Security policy * Security control measures are identified and categorized as per the laws governing security in ICT. | | * Practical * Oral questioning * Written tests | | * Cyber Security, authored by John G. Voeller published by Wiley 2014 |  |
|  | **CAT ONE** | | | | | | | | |
|  | 4 | Establish and install security measures | Types of Security measures   * Firewalls * User accounts control * Security policies * Antivirus * Encryption * Secure Socket Layer protocol (SSL) | * Installation of Security control measures is done as per the ICT Security policy | | * Written tests * Observation * Report writing * Practical | | * Cyber Security, authored by John G. Voeller published by Wiley 2014 |  |
|  | 4 | Establish and install security measures | * Multi-factor authentication * Malware detection * Site monitoring * Daily or weekly backups | * Security control measures are identified and categorized as per the laws governing security in ICT. | | * Written tests * Observation * Report writing * Practical | | * Cyber Security, authored by John G. Voeller published by Wiley 2014 |  |
|  | 4 | Deploy security measures | * Implement security measures contained in the ICT security policy * Apply physical and logical risk mitigation measures | * Implement security measures contained in the ICT security policy * Apply physical and logical risk mitigation measures | | * Practical * Oral questioning * Short tests to assess underpinning knowledge. | | <http://icta.go.ke/national-ict-policy/>  : https://[www.computerworld.com/article/2572970/10-steps-to-](http://www.computerworld.com/article/2572970/10-steps-to-) a-successful-security-policy.html |  |
|  | 4 | Deploy security measures | * Take corrective action * Security audit to identify security gaps * Generate system audit report | * Take corrective action * Security audit to identify security gaps * Generate system audit report | | * Practical * Oral questioning * Short tests to assess underpinning knowledge. | | <http://icta.go.ke/national-ict-policy/>  : https://[www.computerworld.com/article/2572970/10-steps-to-](http://www.computerworld.com/article/2572970/10-steps-to-) a-successful-security-policy.html |  |
|  | **REVISION AND EXAMS** | | | | | | | | |

CHECKED BY VERIFIED BY:

NAME: NAME:

DESIGNATION DESIGNATION