COMPETENCY STANDARD

FOR

Penetration Testing

(Cyber Security)

ICT Sector

Level: 4

Competency Standard Code: ICTCS0004L4V1

National Skills Development Authority
Prime Minister's Office, Bangladesh

Contents

Introduction

The National Skills Development Authority (NSDA) aims to enhance an individual's employability by certifying completeness with skills. NSDA works to expand the skilling capacity of identified public and private training providers qualitatively and quantitatively. It also aims to establish and operationalize a responsive skill ecosystem and delivery mechanism through a combination of well-defined set of mechanisms and necessary technical supports.

Key priority economic growth sectors identified by the government have been targeted by NSDA to improve current job skills along with existing workforce to ensure required skills to industry standards. Training providers are encouraged and supported to work with industry to address identified skills and knowledge to enable industry growth and increased employment through the provision of market responsive inclusive skills training program. **Penetration Testing (Cyber Security)** is selected as one of the priority occupations of **Information and Communication Technology** Sector. This standard is developed to adopt a demand driven approach to training with effective inputs from Industry Skills Councils (ISC's), employer associations and employers.

Generally, a competency standard informs curriculum, learning materials, assessment and certification of students enrolled in TVET. Students who successfully pass the assessment will receive a qualification in the National Skills Qualification Framework (NSQF) and will be listed on the NSDA's online portal.

This competency standard is developed to improve skills and knowledge in accordance with the job roles, duties and tasks of the occupation and ensure that the required skills and knowledge are aligned to industry requirements. A series of stakeholder consultations, workshops were held to develop this document.

The document also details the format, sequencing, wording and layout of the Competency Standard for an occupation which is comprised of Units of Competence and its corresponding Elements.

Overview

A **competency standard** is a written specification of the knowledge, skills and attitudes required for the performance of an occupation, trade or job corresponding to the industry standard of performance required in the workplace.

The purpose of a competency standards is to:

- provide a consistent and reliable set of components for training, recognising and assessing people's skills, and may also have optional support materials
- enable industry recognised qualifications to be awarded through direct assessment of workplace competencies
- encourage the development and delivery of flexible training which suits individual and industry requirements
- encourage learning and assessment in a work-related environment which leads to verifiable workplace outcomes

Competency standards are developed by a working group comprised of representative from NSDA, Key Institutions, ISC, and industry experts to identify the competencies required of an occupation in **Information and Communication Technology** sector.

Competency standards describe the skills, knowledge and attitude needed to perform effectively in the workplace. CS acknowledge that people can achieve technical and vocational competency in many ways by emphasizing what the learner can do, not how or where they learned to do it.

With competency standards, training and assessment may be conducted at the workplace or at training institute or any combination of these.

Competency standards consist of a number of units of competency. A unit of competency describes a distinct work activity that would normally be undertaken by one person in accordance with industry standards.

Units of competency are documented in a standard format that comprises of:

- unit title
- nominal duration
- unit code
- unit descriptor
- elements and performance criteria
- variables and range statement
- curricular content guide
- assessment evidence guide

Together, all the parts of a unit of competency:

- describe a work activity
- guide the assessor to determine whether the candidate is competent or not yet competent

The ensuing sections of this document comprise of a description of the relevant occupation, trade or job with all the key components of a unit of competency, including:

- a chart with an overview of all Units of Competency for the relevant occupation, trade or job including the Unit Codes and the Unit of Competency titles and corresponding Elements
- the Competency Standard that includes the Unit of Competency, Unit Descriptor, Elements and Performance Criteria, Range of Variables, Curricular Content Guide and Assessment Evidence Guide

Level descriptors of NTVQF/ NSQF (BNQF 1-6)

Level & Job classification	Knowledge Domain	Skills Domain	Responsibility Domain
6 Mid-Level Manager/ Sub Assistant Engineer	Comprehensive actual and theoretical knowledge within a specific work or study area with an awareness of the validity and limits of that knowledge, able to analyze, compare, relate and evaluate.	Specialised and wider range of cognitive and practical skills required to provide leadership in the development of creative solutions to defined problems. Communicate professional issues and solutions to the team and to external partners/users.	Work under broad guidance and self-motivation to execute strategic and operational plan/s. Lead lower-level management. Diagnose and resolve problems within and among work groups.
5 Supervisor	Broad knowledge of the underlying, concepts, principles, and processes in a specific work or study area, able to scrutinize and break information into parts by identifying motives or causes.	Broad range of cognitive and practical skills required to generate solutions to specific problems in one or more work or study areas. Communicate practice-related problems and possible solutions to external partners.	Work under guidance of management and self-direction to resolve specific issues. Lead and take responsibility for the work and actions of group/team members. Bridge between management.
4 Highly Skilled Worker	Broader knowledge of the underlying, concepts, principles, and processes in a specific work or study area, able to solve problems to new situations by comparing and applying acquired knowledge.	A range of cognitive and practical skills required to accomplish tasks and solve problems by selecting and applying the full range of methods, tools, materials and information. Communicate using technical terminology and IT technology with partners and users as per workplace requirements.	Work under minimal supervision in specific contexts in response to workplace requirements. Resolve technical issues in response to workplace requirements and lead/guide a team/ group.
3 Skilled Worker	Moderately broad knowledge in a specific work or study area, able to perceive ideas and abstract from drawing and design according to workplace requirements.	Basic cognitive and practical skills required to use relevant information in order to carry out tasks and to solve routine problems using simple rules and tools. Communicate with his team and limited external partners upholding the values, nature and culture of the workplace	Work or study under supervision with considerable autonomy. Participate in teams and responsible for group coordination.
2 Semi-Skilled Worker	Basic understanding of underpinning knowledge in a specific work or study area, able to interpret and apply common occupational terms and instructions.	Skills required to carry out simple tasks, communicate with his team in the workplace presenting and discussing results of his work with required clarity.	Work or study under supervision in a structured context with limited scope of manipulation
1 Basic Skilled Worker	Elementary understanding of ability to interpret the underpinning knowledge in a specific study area, able to interpret common occupational terms and instructions.	Specific Basic skills required to carry out simple tasks. Interpret occupational terms and present the results of own work within guided work environment/ under supervision.	Work under direct supervision in a structured context with limited range of responsibilities.

List of Abbreviations

General

NSDA - National Skills Development Authority

CS – Competency Standard

ILO – International Labor Organization

ISC – Industry Skills Council

NSQF – National Skills Qualifications Framework

BNQF – Bangladesh National Qualifications Framework

NTVQF – National Technical and Vocational Qualifications Framework

SCVC – Standards and Curriculum Validation Committee

TVET – Technical Vocational Education and Training

UoC – Unit of Competency

Occupation Specific Abbreviations

MSDS – Material Safety Data Sheet

OSH – Occupational Safety and Health

PPE – Personal Protective Equipment

SOP – Standard Operating Procedures

Approval of Competency Standard

Members of the Approval Committee:

Member	Signature
Dulal Krishna Saha Executive Chairman (Secretary) National Skills Development Authority (NSDA)	21.06.21
Md. Nurul Amin Member (Admin & Finance) And Member (Registration & Certification) Joint Secretary National Skills Development Authority (NSDA)	21.06.21
Alif Rudaba Member (Planning & Skills Standard) Joint Secretary National Skills Development Authority (NSDA)	

21.06.21

Dulal Krishna Saha

Executive Chairman (Secretary)

National Skills Development Authority (NSDA)

Competency Standards for National Skill Certificate –4 in Penetration Testing (Cyber Security) in ICT Sector

Course Structure

SL	Unit Code and Title		UoC Level	Nominal Duration (Hours)
The Generic Competencies				**30**
1	GU002L2V1	Apply Occupational Safety and Health (OSH) practices in the workplace	1	15
2	GU005L3V1	Carry out workplace interaction in English	3	15
The Sector Specific Competencies				**70**
1	SUICT001L2V1	Operate a Personal Computer and Use Application programs	2	15
2	SUICT002L2V1	Operate office application software	2	25
3	SUICT003L3V1	Access Information using Internet and electronic mail	3	15
4	SUICT004L3V1	Comply to Ethical Standards in IT Workplace	3	15
The Occupation Specific Competencies				**260**
1	OUCyS001L4V!	Interpret Information Security Concepts	4	20
2	OUCyS013L4V!	Apply Programming Concepts	4	30
3	OUCyS002L4V!	Apply Operating Systems Administration Concepts	4	25
4	OUCyS003L4V!	Analyze malicious code	4	30
5	OUCyS004L4V!	Apply Web Application Security	4	50
6	OUCyS007L4V!	Apply the Techniques of Web services Hacking	4	25
7	OUCyS009L4V!	Apply Vulnerability Assessment	4	60
8	OUCyS008L4V!	Apply Information Security Systems Bypass	4	20
Total Nominal Learning Hours				**360**

Units & Elements at a glance

Generic Competencies

Code	Unit of Competency	Elements of Competency	Nominal Hours
GU002L2V1	Apply Occupational Safety and Health (OSH) Practices in the Workplace	1. Identify OSH policies and procedures 2. Follow OSH procedures 3. Report hazards and risks 4. Respond to emergencies 5. Maintain personal well-being	15
GU005L3V1	Carry out workplace interaction in English	1. Interpret workplace communication and etiquette 2. Read and Understand Workplace Documents 3. Participate in workplace meetings and discussions 4. Practice professional ethics at workplace	15

Sector Specific Competencies

Code	Unit of Competency	Elements of Competency	Nominal Hours
SUICT001L2V1	Operate a Personal Computer and Use Application programs	1. Start computer 2. Access basic system information 3. Work with files and folders 4. Use application programs 5. Print documents 6. Shut down computer	15
SUICT002L2V1	Operate office application software	1. Operate computer 2. Install application software 3. Use word processor to prepare/create documents 4. Use spreadsheet to create /prepare worksheets 5. Use presentation software to create / prepare presentation 6. Print a document	25
SUICT003L3V1	Access Information using Internet and electronic mail	1. Access resources from internet 2. Use and manage Electronic mail 3. Use audio/video tools for information transfer	15
SUICT004L3V1	Comply to Ethical Standards in IT Workplace	1. Uphold the requirements of clients 2. Deliver quality products and services 3. Maintain professionalism at workplace 4. Maintain workplace code of conduct.	15

The Occupation Specific Competencies

Code	Unit of Competency	Elements of Competency	Duration (Hours)
OUCyS001L4V!	Interpret Information Security Concepts	1. Interpret Information Security System 2. Interpret Hacking Techniques 3. Identify types of Attacks 4. Categorize Security Threats & Control 5. Interpret Cyber Law	20
OUCyS013L4V!	Apply Programming Concepts	1. Interpret Programming Concepts 2. Use HTML and CSS 3. Use Power Shell 4. Apply Shell Scripts	30
OUCyS002L4V!	Apply Operating Systems Administration Concepts	1. Install Virtual machine 2. Install OS 3. Perform Hacking using hacking tool	25
OUCyS003L4V!	Analyze malicious code	1. Interpret Malicious Code 2. Identify malwares 3. Analyze Malicious Code using Tools 4. Countermeasures for Malware infections	30
OUCyS004L4V!	Apply Web Application Security	1. Interpret Web Application Security 2. Perform web application penetration testing 3. Perform web application countermeasures	50
OUCyS007L4V!	Apply the Techniques of Web services Hacking	1. Identify Web server Vulnerabilities 2. Analyze web application 3. Identify Web Application Threats & Attack 4. Apply Session Hijacking 5. Insufficient logging and monitoring	25
OUCyS009L4V!	Apply Vulnerability Assessment	1. Interpret vulnerability concept 2. Use Vulnerability Assessment tools 3. Prepare VA Report	60
OUCyS008L4V!	Apply Information Security Systems Bypass	1. Interpret Information Security Systems Bypass 2. Analyze Security Solutions to identify Vulnerabilities 3. Use Tools to Bypass the Security Solutions	20

The Generic Competencies

Unit Code and Title	**GCU02L2V1: Apply Occupational Safety and Health (OSH) Procedure in the Workplace**
Nominal Hours	**15 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes (KSA) required in applying occupational safety and health (OSH) procedures in the workplace. It specifically includes the tasks of identifying OHS policies and procedures, following OSH procedure, reporting to emergencies, and maintaining personal well-being.
Elements of Competency	**Performance Criteria** **Bold & Underlined** terms are elaborated in the Range of Variables
1. Identify OSH policies and procedures.	1.1. **OHS policies** and **safe operating procedures** are accessed and stated. 1.2. **Safety signs and symbols** are identified and followed. 1.3. Emergency response, evacuation procedures and other contingency measures are determined according to workplace requirements.
2. Follow OSH procedure	2.1 **Personal protective equipment (PPE)** is selected and collected as required. 2.2 Personal protective equipment (PPE) is correctly used in accordance with organization OHS procedures and practices. 2.3 A clear and tidy workplace is maintained as per workplace standard. 2.4 PPE is maintained to keep them operational and compliant with OHS regulations.
3. Report hazards and risks.	3.1 **Hazards** and risks are identified, assessed and controlled. 3.2 Incidents arising from hazards and risks are reported to designated authority.
4. Respond to emergencies	4.1 Alarms and warning devices are responded. 4.2 Workplace **emergency procedures** are followed. 4.3 **Contingency measures** during workplace accidents, fire and other emergencies are recognized and followed in accordance with organization procedures. 4.4 Frist aid procedures is applied during emergency situations.
5. Maintain personal well-being	5.1 OHS policies and procedures are adhered to. 5.2 OHS awareness programs are participated in as per workplace guidelines and procedures. 5.3 Corrective actions are implemented to correct unsafe condition in the workplace. 5.4 **"Fit to work" records** are updated and maintained according to workplace requirements.
Range of Variables	
Variables	**Range** (may include but not limited to):

1. OHS Policies	1.1. Bangladesh standards for OHS 1.2. Fire Safety Rules and Regulations 1.3. Code of Practice 1.4. Industry Guidelines
2. Safe Operating Procedures	2.1 Orientation on emergency exits, fire extinguishers, fire escape, etc. 2.2 Emergency procedures 2.3 First Aid procedures 2.4 Tagging procedures 2.5 Use of PPE 2.6 Safety procedures for hazardous substances
3. Safety Signs and symbols	3.1 Direction signs (exit, emergency exit, etc.) 3.2 First aid signs 3.3 Danger Tags 3.4 Hazard signs 3.5 Safety tags 3.6 Warning signs
4. Personal Protective Equipment (PPE)	4.1 Gas Mask 4.2 Gloves 4.3 Safety boots 4.4 Face mask 4.5 Overalls 4.6 Goggles and safety glasses 4.7 Sun block 4.8 Chemical/Gas detectors
5. Hazards	5.1 Chemical hazards 5.2 Biological hazards 5.3 Physical Hazards 5.4 Mechanical and Electrical Hazard 5.5 Mental hazard 5.6 Ergonomic hazard
6. Emergency Procedures	6.1 Fire fighting 6.2 Earthquake 6.3 Medical and first aid 6.4 evacuation`
7. Contingency measures	7.1 Evacuation 7.2 Isolation 7.3 Decontamination
8. “Fit to Work” records	8.1 Medical Certificate every year 8.2 Accident reports, if any 8.3 Eye vision certificate

Evidence Guide
The evidence must be authentic, valid, sufficient, reliable, consistent, recent and meet all requirements of current version of the Unit of Competency

1. Critical aspects of competency	Assessment required evidence that the candidate: 1.1 stated OHS policies and safe operating procedures 1.2 followed safety signs and symbols

	1.3 used personal protective equipment (PPE) 1.4 maintained workplace clear and tidy 1.5 assessed and Controlled hazards 1.6 followed emergency procedures 1.7 followed contingency measures 1.8 implemented corrective actions
2. Underpinning knowledge	2.1 Define OHS 2.2 OHS Workplace Policies and Procedures 2.3 Work Safety Procedures 2.4 Emergency Procedures 2.5 Hazard control procedure 2.6 Different types of Hazards 2.7 PPE and there uses 2.8 Personal Hygiene Practices 2.9 OHS Awareness
3. Underpinning skills	3.1 Accessing OHS policies 3.2 Handling of PPE 3.3 Handling cleaning tools and equipment 3.4 Writing report 3.5 Responding to emergency procedures
4. Required attitude	4.1 Commitment to occupational health and safety 4.2 Sincere and honest to duties 4.3 Promptness in carrying out activities 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect of peers and seniors in workplace 4.8 Communicate with peers and seniors in workplace
5. Resource implications	5.1 Adequate workplace 5.2 Equipment and outfits appropriate in applying safety measures 5.3 Tools, materials and documentation required 5.4 OHS Policies and Procedures
6. Methods of assessment	6.1 Written test 6.2 Demonstration 6.3 Oral Questioning 6.4 Portfolio
7. Context of assessment	7.1 Competency assessment must be done in NSDA accredited assessment centre 7.2 Assessment should be done by a NSDA certified/nominated assessor.

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**GU005L3V1: Carryout Workplace Interaction in English**
Nominal Hours	**15 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to carry out workplace interaction. It specifically includes – interpreting workplace communication and etiquette; reading and understand workplace documents; participating in workplace meetings and discussions; and practicing professional ethics at workplace.
Elements of Competency	**Performance Criteria** **Bold & Underlined** terms are elaborated in the Range of Variables Training Components
1. Interpret workplace communication and etiquette	1.1 Workplace code of conducts are interpreted as per organizational guidelines 1.2 Appropriate lines of communication are maintained with supervisors and colleagues 1.3 Workplace interactions are conducted in a **courteous manner** to gather and convey information 1.4 Questions about routine **workplace procedures and matters** are asked and responded as required
2. Read and Understand Workplace Documents	2.1 Workplace documents are interpreted as per standard. 2.2 Assistance is taken to aid comprehension when required from peers / supervisors 2.3 Visual information / symbols / signage's are understood and followed 2.4 Specific and relevant information are accessed from **appropriate sources** 2.5 Appropriate medium is used to transfer information and ideas
3. Participate in workplace meetings and discussions	3.1 Team meetings are attended on time and followed meeting procedures and etiquette 3.2 Own opinions are expressed and listened to those of others without interruption 3.3 Inputs are provided consistent with the meeting purpose and interpreted and implemented meeting outcomes
4. Practice professional ethics at workplace	4.1 Responsibilities as a team member are demonstrated and kept promises and commitments made to others 4.2 Tasks are performed in accordance with workplace procedures 4.3 Confidentiality is respected and maintained 4.4 Situations and actions considered inappropriate or which present a conflict of interest are avoided

Range of Variables	
Variable	**Range** (may include but not limited to):
1. Courteous Manner	1.1 Effective questioning 1.2 Active listening 1.3 Speaking skills
2. Workplace Procedures and Matters	2.1 Notes 2.2 Agenda 2.3 Simple reports such as progress and incident reports 2.4 Job sheets 2.5 Operational manuals 2.6 Brochures and promotional material 2.7 Visual and graphic materials 2.8 Standards 2.9 OSH information 2.10 Signs
3. Appropriate Sources	3.1 HR Department 3.2 Managers 3.3 Supervisors
Evidence Guide The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency	
1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 followed workplace code of conducts is as per organizational guidelines 1.2 interpreted workplace documents as per standard 1.3 interpreted workplace instructions and symbols 1.4 interpreted and implemented meeting outcomes
2. Underpinning Knowledge	2.1 Workplace communication and etiquette 2.2 Workplace documents, signs and symbols 2.3 Meeting procedure and etiquette
3. Underpinning Skills	3.1 Demonstrating performance of workplace communication and etiquette 3.2 Following workplace instructions and symbol 3.3 Following workplace code of conducts is as per organizational guidelines 3.4 Interpreting workplace documents as per standard 3.5 Interpreting and implementing meeting outcomes

4. Underpinning Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	6.1 Written Test 6.2 Demonstration 6.3 Oral Questioning 6.4 Portfolio
7. Context of Assessment	7.1 Competency assessment must be done in NSDA accredited center. 7.2 Assessment should be done by NSDA certified/ nominated assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

The Sector Specific Competencies

Unit Code and Title	**SUICT001L3V1: Operate a Personal Computer and Use Applications Programs**
Nominal Hours	**15 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to operate a personal computer and use applications programs. It specifically includes starting computer, accessing basic system information, working with files and folders, using application programs, printing documents and shutting down computer.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables Training Components
1. Start computer	1.1 Safe workplace practices are observed according to IT workplace guideline. 1.2 Computer is checked for proper connection position and usability. 1.3 **Peripheral devices** are checked for correct connection, position and usability. 1.4 Power of computer and other peripheral devices are switched on.
2. Access basic system information	2.1 User name and password as prompted and note access, privacy, security and related conditions of use displayed on introductory screens are inserted. 2.2 PC desktop environment/Graphical User Interface_(GUI) settings is arranged and customized. 2.3 The **operating system** information is identified. 2.4 System configuration and application versions in operation are navigated.
3. Work with files and folders	3.1 Desktop environment is customized. 3.2 Basic directory and sub-directories are created and named. 3.3 Attributes of directories are identified. 3.4 Files for user and organization requirements are created and organized 3.5 Data are entered into the desired office application in accordance with work requirements 3.6 Files are copied and saved to available **data storage devices.**
4. Use application programs	4.1 Calculator program is used 4.2 Notepad is used 4.3 WordPad is used 4.4 Snipping Tool is applied 4.5 Paint is used 4.6 Sticky Note is used

5. Print documents	5.1 Printer settings, if required, are entered into the program 5.2 Default printer is changed where necessary 5.3 Print preview option is accessed to effect printing of documents 5.4 Adjust document print output where necessary 5.5 Printout is taken
6. Shut down computer	6.1 All opened files/documents are exited. 6.2 All opened **application programs** are logged out in accordance with standard application procedure. 6.3 Personal computer is shut down in accordance with standard shut down procedure. 6.4 The computer and other peripherals are switched off and switched off power supply in accordance with standard procedure.
Range of Variables	
Variables	**Range** (may include but not limited to):
1. Peripheral devices	1.1 Input Devices 1.1.1 keyboard, MIDI keyboard 1.1.2 mouse 1.1.3 touch screen 1.1.4 Digitizer tablet 1.1.5 joystick 1.1.6 scanner 1.1.7 digital camera 1.1.8 video camera 1.1.9 microphone 1.2 Output Devices 1.2.1 monitor 1.2.2 projector 1.2.3 TV screen 1.2.4 printer 1.2.5 plotter 1.2.6 speakers 1.3 Both input/output 1.3.1 external hard drives 1.3.2 USB drives 1.3.3 media card readers 1.3.4 digital camcorders 1.3.5 digital mixers 1.3.6 MIDI equipment
2. Operating system	2.1 Microsoft Windows 2.2 Apple Mac OS 2.3 Ubuntu Linux 2.4 Google android 2.5 iOS
3. Data storage devices	3.1 Random Access Memory (RAM) 3.2 Hard disk 3.3 CD/DVD 3.4 Flash drive 3.5 External hard disk
Evidence Guide	

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency	
1. Critical aspects of competency	Assessment required evidence that the candidate: 1.1 arranged, customized and manipulated PC desktop environment/graphical user interface (GUI) settings. 1.2 selected, opened and closed desktop icons to access application programs 1.3 entered data into the desired office application in accordance with work requirements 1.4 entered print command to effect printing of documents
2. Underpinning knowledge	2.1 Basic software 2.2 Computer functions 2.3 Creating and opening documents 2.4 Formatting documents 2.5 Inserting tables and images 2.6 Saving, printing and closing documents 2.7 Mail merge function 2.8 Basic keyboarding skills 2.9 Methods and procedure in switching on and off the computer and other peripherals 2.10 Selection, opening and closing procedures of desktop icons to access application programs 2.11 Method of creating and organizing files for user and organization requirements 2.12 Data input techniques in accordance with standard typing procedure and office application 2.13 Printing procedure and commands
3. Underpinning skill	3.1 Switching on power of computer and other peripheral devices 3.2 Arranging, customizing and manipulating PC desktop environment/graphical user interface (GUI) settings 3.3 Selecting, opening and closing desktop icons to access application programs 3.4 Creating and organizing Files for user and organization requirements 3.5 Entering data into the desired office application in accordance with work requirements 3.6 Entering print command to effect printing of documents 3.7 Switching off the computer and other peripherals and unplugging power supply in accordance with standard procedure
4. Required attitude	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace

	4.8 Communication with peers and seniors in workplace
5. Resource implication	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of assessment	6.1 Written Test 6.2 Demonstration 6.3 Oral Questioning 6.4 Portfolio
7. Context of assessment	7.1 Competency assessment must be done in NSDA accredited center. 7.2 Assessment should be done by NSDA certified/ nominated assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**SUICT002L3V1: Operate Office Application Software**
Nominal Hours	**25 hours**
Unit Descriptor	This unit covers the knowledge, skills and attitude required to operate office application software. It specifically includes operating computer, installing application software, using word processor to prepare/create documents, using spread sheet to create /prepare worksheets, using presentation software to create / prepare presentation, and printing a document.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variable Training Components
1. Operate computer	1.1 Safe workplace practices are observed according to IT workplace guideline. 1.2 Desktop **Peripherals** are checked and connected with computer properly. 1.3 Computer is switched on. 1.4 Computer **desktop / GUI settings** are arranged and customized as per requirement. 1.5 Files and folders are **manipulated** as per requirement. 1.6 Properties of files and folders are viewed and searched. 1.7 Disks are defragmented, formatted as per requirement.
2. Install application software	2.1 Installation requirements of software are identified 2.2 and listed. 2.3 Software sources and CD key/ password are assured. 2.4 **Appropriate Software** are collected and selected as 2.5 per requirement. 2.6 Software installation is started. 2.7 Customization is done as per requirement. 2.8 Steps of installation are followed as per installation Instructions. 2.9 Installations are completed properly. 2.10 Correctness of Installation is checked.
3. Use word processor to prepare/create documents	3.1 Appropriate **word processor** is Selected and started. 3.2 Documents are created as per requirement in Personal use and office environment. 3.3 Contents are entered. 3.4 Documents are formatted. 3.5 Paragraph and page settings are completed. 3.6 Document is saved.
4. Use spreadsheet to create /prepare worksheets	4.1 **Spreadsheet applications** are selected and started. 4.2 Worksheets are created as per requirement in Personal use and office environment. 4.3 Data are entered 4.4 Functions are used for calculating and editing logical operation 4.5 Sheets are formatted as per requirement. 4.6 Charts are created. 4.7 Charts/ Sheets are saved.
5. Use presentation software to create / prepare presentation	5.1 Appropriate **presentation applications** are selected and started 5.2 Presentation is created as per requirement in personal use and office environment

	5.3 Image, Illustrations, text, table, symbols and media are entered as per requirements. 5.4 Presentations are formatted and animated. 5.5 Presentations are viewed and saved.
6. Print a document	6.1. Printer is connected with computer. 6.2. Power is switched on at both the power outlet and printer. 6.3. Printer is installed and added. 6.4. Paper of proper size is put into printer. 6.5. Correct printer setting is selected 6.6. Document is previewed and printed. 6.7. Print from the printer spool is viewed or cancelled and unsaved data is saved as per requirements. 6.8. Opened software is closed. 6.9. Devices are shut down.

Range of Variables

Variable	**Range** (May include but not limited to:)
1. Peripherals	1.1 Monitor 1.2 Keyboard 1.3 Mouse 1.4 Modem 1.5 Scanner 1.6 Printer
2. Desktop/ GUI settings	2.1 Icons 2.2 Taskbar 2.3 View 2.4 Resolutions
3. Manipulate	3.1 Create 3.2 Open 3.3 Copy 3.4 Rename 3.5 Delete 3.6 Sort
4. Appropriate Software	5.1 Word processor. 5.2 Spread sheet application. 5.3 Presentation application.
5. Word processor	6.1 MS Word processor 6.2 Open office Org 6.3 Google docs 6.4 Word perfect 6.5 LibreOffice
6. Spread sheet applications	7.1 MS Excel 7.2 Google Sheets 7.3 Apple Numbers by Apple
7. Presentation application	8.1 MS PowerPoint 8.2 Google Slides 8.3 Prezi

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency.

1. Critical aspects of competency	Assessment required evidence that the candidate: 1.1 installed Operating system 1.2 manipulated Files and folders as per requirement 1.3 installed application software 1.4 used functions in spread sheet. 1.5 applied animations into presentation slide.

	1.6 printed document.
2. Underpinning knowledge	2. 1 Desktop items 2. 2 Type of Bangla keyboard layout 2. 3 Different type of software and application packages 2. 4 Use of word processor, spread sheet and presentation software 2. 5 Type of printers 2. 6 Type of charts, Impotence of chart 2. 7 Different type of math and logical functions.
3. Underpinning skill	3.1 Starting computer 3.2 Installing Operating system 3.3 Managing desktop item 3.4 Manipulating Files and folders as per requirement 3.5 Installing application software 3.6 Running application software 3.7 Creating and saving document with word processing application. 3.8 Using functions in spread sheet. 3.9 Applying animations into presentation slide. 3.10 Printing document.
4. Required attitude	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers, sub-ordinates and seniors in workplace
5. Resource implication	Following Resources must be provided 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of assessment	6.1 Written Test 6.2 Demonstration 6.3 Oral Questioning 6.4 Portfolio
7. Context of assessment	7.1. Competency assessment must be done in NSDA accredited center. 7.2. Assessment should be done by NSDA certified/ nominated assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the national quality assurance body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any national qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**SUICT003L3V1: Access Information using Internet and Electronic mail**
Nominal Hours	**15 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitude required to access information using internet and electronic mail. It specifically includes accessing resources from internet, using and managing electronic mail, and using audio/video tools for information transfer.
Elements of Competency	**Performance Criteria** **Bold and underlined** terms are elaborated in the Range of Variable.
1. Access resources from internet	1.1 Appropriate internet **browsers** are selected and installed. 1.2 Internet browser is opened and web address / URL is written/selected in /from address bar to access **information.** 1.3 **Search engines** are used to access information 1.4 Video / Information are Shared /downloaded / uploaded from / to web site/**social media**. 1.5 **Web based resources** are used. 1.6 Netiquette' (or web etiquette) principles are searched and followed.
2. Use and manage electronic mail	2.1. **Email services** are identified and selected to create a new email address 2.2. Email account is created. 2.3. Document is prepared, attached and sent to different types of recipient. 2.4. Email is read, forwarded, replied and deleted as per requirement. 2.5. Custom email folders are created and manipulated. 2.6. Email message is printed.
3. Use audio/video tools for information transfer	3.1 Audio and video tools are identified 3.2 Apps using audio/video tools are identified 3.3 Information is transferred with apps using audio/video tools
Range of Variables	
Variable	**Range** (May include but not limited to:)
1. Browsers	1.1 Mozilla Firefox 1.2 Google chrome 1.3 Internet explorer 1.4 Opera
2. Information	2.1. Text information 2.2. Graphics 2.3. Video
3. Search engines	3.1. Google 3.2. Yahoo 3.3. AltaVista 3.4. Msn 3.5. Bing
4. Social media.	4.1 Face book 4.2 Twitter

	4.3 LinkedIn 4.4 YouTube
5. Web based services	5.1 Drive 5.2 Calendar 5.3 Map 5.4 Translator 5.5 Docs 5.6 search
6. Email services	6.1 Free mail services –Gmail, Yahoo, Hotmail 6.2 Web mail services.

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency.

1. Critical aspects of competency	Assessment required evidence that the candidate: 1.1 downloaded / uploaded video / Information from / to web site 1.2 prepared, attached and sent documents to different types of recipient.
2. Underpinning knowledge	2.1. Internet 2.2. www 2.3. web site 2.4. web address 2.5. URL 2.6. Web browsers 2.7. Search engines 2.8. Information 2.9. Social media 2.10. Web based services 2.11. Folder manipulation
3. Underpinning skill	3.1 Accessing and sharing resources from internet 3.2 Downloading /uploading file, documents and video from /to web sites 3.3 Sending and receiving mail through mail service. 3.4 Using audio/video tools to share information.
4. Required attitude	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers, sub-ordinates and seniors in workplace
5. Resource implication	Following Resources must be provided- 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of assessment	6.1 Written Test 6.2 Demonstration 6.3 Oral Questioning 6.4 Portfolio

7. Context of assessment	7.1. Competency assessment must be done in NSDA accredited center. 7.2. Assessment should be done by NSDA certified/ nominated assessor
Accreditation Requirements Training Providers must be accredited by National Skills Development Authority (NSDA), the national quality assurance body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any national qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.	

Unit Code and Title	**SUICT004L3V1: Comply to Ethical Standards in IT Workplace**
Nominal Hours	**15 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to comply to ethical standards in IT workplace. It specifically includes upholding the requirements of clients, delivering quality products and services, maintaining professionalism at workplace, and maintaining workplace code of conduct.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Uphold the requirements of clients	1.1 Clients' requirements are identified. 1.2 Confidentiality of information is maintained in accordance with workplace policies / organizational policies/ national legislation. 1.3 Potential conflicts of interest are identified and involved parties of potential conflicts are notified. 1.4 Proprietary rights of client/customer is asserted.
2. Deliver quality products and services	2.1. Products and services are provided according to the clients' requirements. 2.2. Work is completed as per standards. 2.3. Quality processes are implemented when developing products and services.
3. Maintain professionalism at workplace	3.1 Work processes are delivered as per standards. 3.2 Skills, knowledge and qualifications are presented in a professional manner. 3.3 Services and products developed by self and others are delivered as per workplace standard. 3.4 Unbiased and objective information are provided to clients. 3.5 Realistic estimates for time, cost and delivery of outputs are presented during negotiation.
4. Maintain workplace code of conduct.	4.1 Workplace code of conduct are interpreted 4.2 Workplace code of conduct is followed.
Range of variables	
Variables	**Range** (may include but not limited to):
Evidence Guide The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency	
1. Critical aspects of competency	Assessment required evidence that the candidate: 1.1 asserted proprietary rights of client/customer. 1.2 completed work to industry and international standards. 1.3 implemented quality processes when developing products and services.

	1.4 delivered services and products developed by self and others. 1.5 provided unbiased and objective information to clients. 1.6 followed workplace code of conduct.
2. Underpinning knowledge	2.1. Corporate code of confidentiality of information 2.2. organizational policies, national legislation and workplace policies in relation to IT sector 2.3. Law and regulations pertaining to proprietary rights 2.4. Quality processes for products and services 2.5. Procedure of provided to client information 2.6. Method of estimating for time, cost and delivery products and services 2.7. Workplace code of conduct in IT sector
3. Underpinning Skills	3.1. Upholding confidentiality of information in accordance with organizational policies, national legislation and workplace policies 3.2. Asserting proprietary rights of client/customer 3.3. Completing work in accordance with industry and international standards 3.4. Implementing quality processes when developing products and services 3.5. Delivering correctly services and products developed by self and others 3.6. Providing unbiased and objective information are to clients. 3.7. Presenting realistic estimates for time, cost and delivery of outputs during negotiation 3.8. Following workplace code of conduct
4. Underpinning Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace.
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	6.1 Written Test 6.2 Demonstration 6.3 Oral Questioning 6.4 Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in NSDA accredited center. 7.2. Assessment should be done by NSDA certified/ nominated assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

The Occupation Specific Competencies

Unit Code and Title	**OUCyS001L4V1: Interpret Information Security Concepts**
Nominal Hours	**20 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to interpret information security concepts in the workplace. It specifically includes the tasks of interpreting information security system, hacking techniques, identifying types of attacks, categorizing security threats & control and interpreting cyber law.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret Information Security System	1.1 Information Security is interpreted;
	1.2 Information **Security Principles** are stated;
	1.3 Information Security Policy is interpreted;
	1.4 Information **security framework** are listed;

2. Interpret Hacking Techniques	2.1 Hacking is Interpreted;
	2.2 **Types of hackers** is identified;
	2.3 Hacking Techniques is Interpreted;

3. Identify types of Attacks	3.1 Step of hacking is interpreted; 3.2 **Types of Attacks** are identified;
4. Categorize Security Threats & Control	4.1 Necessity of awareness about cyber security threats is interpreted; 4.2 Anti-Virus Software is Installed; 4.3 Updated patch is ensured; 4.4 Firewall is used to protect networks; 4.5 Internet Downloads are scanned; 4.6 Regular backups of critical data are ensured;

5. Interpret emerging technology	5.1 Artificial Intelligence is interpreted;
	5.2 Big Data is interpreted;
	5.3 Data Science is interpreted;
	5.4 Machine Learning is interpreted;
	5.5 Machine vision is interpreted;

6. Interpret Cyber Law	6.1 Cyber Law is stated; 6.2 Cyber Law Global Impact is interpreted 6.3 Cyber Law in Bangladesh is interpreted
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Security Principles	1.1 Confidentiality 1.2 Integrity 1.3 Availability 1.4 Authentication 1.5 Non-Repudiation
2. Security framework	2.1 NIST cyber security framework (CSF) 2.2 ISO/IEC 27001/2

	2.3 COBIT 5 2.4 ITIL 2.5 General Data Protection Regulation (GDPR)
3. Types of hackers	3.1 Cyber terrorist 3.2 Black Hat' Hackers 3.3 White Hat' Hackers 3.4 Grey Hat' Hackers 3.5 Hacktivist 3.6 Script kiddies
4. Types of Attacks	4.1 Malware Attack 4.2 Phishing 4.3 SQL Injection Attack 4.4 Cross-Site Scripting (XSS) 4.5 Denial of Service (DoS) 4.6 Session Hijacking and Man-in-the-Middle Attacks 4.7 Credential Reuse 4.8 OWASP top 10

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Interpreted global impact of Cyber Law 1.2 Interpreted Cyber Law in Bangladesh 1.3 Identified types of attacks 1.4 Identified types of hackers;
2. Underpinning Knowledge	2.1 Security Principles 2.2 types of Attacks 2.3 Hacking 2.4 Types of hackers 2.5 Hacking Techniques 2.6 Step of hacking 2.7 types of Attacks 2.8 Cyber Law Global Impact 2.9 Cyber Law in Bangladesh
3. Underpinning Skills	3.1 Installing Anti-Virus Software 3.2 Ensuring Updated Anti-virus software 3.3 Installing Firewall 3.4 Scanning Internet Downloads 3.5 Checking data backups 3.6 Performing folder management
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagemess to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace

5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1 Written Test 6.2 Demonstration 6.3 Oral Questioning 6.4 portfolio
7. Context of Assessment	7.1 Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2 Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS013L5V1: Apply Programming Concepts**
Nominal Hours	**30 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply programming concepts in the workplace. It specifically includes the tasks of interpreting programming concepts, using HTML and CSS, Power Shell and apply shell scripts
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret Programming Concepts	1.1 Programming Language is defined;
	1.2 Programming Languages are classified;
	1.3 Algorithm design techniques are explained;
	1.4 Flowchart is created according to algorithm;
	1.5 **Programming Conditions** are interpreted;
	1.6 Concepts of OOP is interpreted;

2. Apply Programming language concepts	2.1 **Web programming** concepts is interpreted; 2.2 Web programming concepts is applied;

3. Use Power Shell	3.1 Functions of Power Shell are defined;
	3.2 Power Shell modules are used;
	3.3 Problems are identified for scripting;
	3.4 Own Scripting are created;

4. Apply Shell Scripts	4.1 **Shell** Script are created in Linux/Unix; 4.2 Bash Scripts are created and used;; 4.3 .sh file is run in shell Script; 4.4 Applications are run in shell script; 4.5 Scripts are creating and run; 4.6 An application is started as per standard from a shell;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Programming Conditions	1.1 If-else 1.2 For Loop 1.3 While 1.4 Do while 1.5 Switch -case
2. Shells	2. 1 Bash Shell 2. 2 Power Shell 2. 3 Ksh Shell 2. 4 Zsh Shell
3. Web programming	2. 5 HTML 2. 6 CSS 2. 7 Java

	2. 8 PHP

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Created flowchart is according to algorithm; 1.2 Written code is implementing basic HTML operations 1.3 Written code is implementing advanced CSS operations; 1.4 Applied Shell Scripts
2. Underpinning Knowledge	2.1 Example of Scripts 2.2 Algorithm 2.3 HTML 2.4 CSS 2.5 Shell Script
3. Underpinning Skills	3.1 Applying concept of algorithm 3.2 Applying concept of programming 3.3 Applying concept of Shell and Shell Script
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS002L4V1: Apply Operating Systems Administration Concepts**
Nominal Hours	**25 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply operating systems administration concepts. It specifically includes the tasks of installing virtual machine, installing OS and performing hacking using hacking tool.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Install Virtual machine	1.1 Concept is virtualized;
	1.2 **VM** is Selected and collected;
	1.3 VM is Installed following SOP;
	1.4 VM is configured following SOP;

2. Install OS	2.1 Basic operating system concepts is interpreted; 2.2 **OS** is selected and collected; 2.3 OS is Installed following SOP; 2.4 Basic **command** is interpreted; 2.5 Internet and network connectivity is checked; 2.6 OS packages with dependency are updated and upgraded;
3. Perform Hacking using hacking tool	3.1 **Hacking tools** are identified as per requirement; 3.2 Hacking tools are installed; 3.3 Hacking tools with dependency are updated and upgraded;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. VM	1.1 Virtual Machine 1.2 Oracle virtual Box 1.3 VM ware
2. OS	2.1 Windows 2.2 Kali Linux 2.3 Ubuntu 2.4 MAC 2.5 Parrot OS
3. Hacking tools	3.1 The harvester 3.2 Nmap 3.3 Wire shirk 3.4 John the ripper 3.5 Responder 3.6 Hashcat 3.7 Metasploit 3.8 Burpsuite

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Configured VM 1.2 Installed OS 1.3 Installed hacking tools
2. Underpinning Knowledge	2.1 Internet 2.2 Basic networking 2.3 NAT 2.4 Local host 2.5 Bridge 2.6 Virtual Machine
3. Underpinning Skills	3.1 Installing OS 3.2 Connecting OS with network 3.3 Checking network connectivity
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1 Written Test 6.2 Demonstration 6.3 Oral Questioning 6.4 portfolio
7. Context of Assessment	7.1 Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2 Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS003L4V1: Analyze Malicious Code**
Nominal Hours	**30 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to analyze malicious code. It specifically includes the tasks of interpreting malicious code, identifying malwares, analyzing malicious code using tools and counter measuring for malware infections.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret Malicious Code	1.1 **Malware** is defined;
	1.2 Threatens of Malicious Code is explained;
	1.3 Process to Avoid Malicious Code is interpreted;
	1.4 Malware propagation techniques is interpreted;

2. Create malwares	2.1 Virus Tools are Selected; 2.2 Program is unzipped as required; 2.3 **Process of malwares infection** is identified; 2.4 Malwares are created using required **tools;** 2.5 Malwares are detected using required tools;
3. Analyze Malicious Code using Tools	3.1 Infected systems is analyzed; 3.2 Malicious code is analyzed using required tools;
4. Implement countermeasures for Malware infections	4.1 Anti-malware is used to prevent malware; 4.2 Countermeasures for Malware infections are selected; 4.3 Selected countermeasures are implemented; 4.4 Malware is removed;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Malware	1.1 Trojans 1.2 Trojan and Backdoors 1.3 Ransomware 1.4 Addware 1.5 Spyware 1.6 Virus 1.7 Worms 1.8 Rootkit
2. Process of malwares infection	2.1 Email attachment 2.2 Drive by download 2.3 Social media
3. Tools	Creation Tools: 3.1 Metasploit 3.2 Poison virus 3.3 Prorat 3.4 SMS-Flooder 3.5 IM-Flooder

	Detection Tools: 3.1 MALWARE CORPORA 3.2 Virustotal.com 3.3 ID serve 3.4 Telosintelligence.com
Evidence Guide The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency	
1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Identified process of malwares infection; 1.2 Detected Malwares by using required tools 1.1 Used Anti-malware to prevent malware 1.2 Implemented selected countermeasures
2. Underpinning Knowledge	2.1. Malware 2.2. Anti-malware 2.3. Phishing 2.4. Vishing 2.5. Smhishing 2.6. Social Engineering
3. Underpinning Skills	3.1 Installing Anti malware tools 3.2 Installing Malware detection tools
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio

7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS004L4V1: Apply Web Application Security**
Nominal Hours	**50 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply web application security. It specifically includes the tasks of interpreting web application security, performing web application penetration testing and web application countermeasures.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret Web Application Security	1.1 Web Application Security is interpreted;
	1.2 OWASP top 10 is interpreted;
	1.2 Web application vulnerabilities are interpreted;
	1.3 Web application firewall (WAF) is interpreted;
	1.4 Web application security checklist is inferred;

2. Perform web application penetration testing	2.1 **Penetration testing steps** are interpreted;
	2.2 Penetration testing is performed using **tools;**
	2.3 Report is prepared;

3. Perform web application countermeasures	3.1 Start with thought like an attacker; 3.2 Web application security is performed using required **Solutions;** 3.3 Network security is performed using required solutions; 3.4 Host security is performed using required Solutions;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Penetration testing steps	1.1 Information gathering 1.2 Scanning 1.3 Enumeration 1.4 Vulnerability Assessment 1.5 Penetrate the application vulnerabilities
2. Tools	2.1 Burp suite 2.2 Acunetix 2.3 Nessus 2.4 Ettercap 2.5 Vega 2.6 Metasploit 2.7 Hashcat 2.8 Medusa 2.9 Netstumdulm 2.10 Zenmap, Cain & Abel

	2.11 Nmap, 2.12 Shodan, 2.13 DNS Forward And Reverse Lookup, 2.14 DNS Zone Transfer, 2.15 Identifying Related External Sites, 2.16 Inspect HEAD and OPTIONS HTTP requests Archive.org
3. Solutions	3.1 Web application firewall 3.2 NGFW 3.3 Application visibility 3.4 URL filtering 3.5 Virtual patching 3.6 Anti-malware protection

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Used web penetration testing tools 1.2 Performed penetration testing is using tools 1.3 Performed network and host security using required solutions
2. Underpinning Knowledge	2.7. Concept of web application security, vulnerabilities and firewall 2.8. Concept of penetration testing 2.9. Steps of VAPT
3. Underpinning Skills	3.3 Programming web application 3.4 Applying vulnerabilities 3.5 Applying knowledge attacker
4. Required Attitudes	4.9 Commitment to occupational health and safety 4.10 Promptness in carrying out activities 4.11 Sincere and honest to duties 4.12 Environmental concerns 4.13 Eagerness to learn 4.14 Tidiness and timeliness 4.15 Respect for rights of peers and seniors in workplace 4.16 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.3 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.4 Required learning materials.

6. Methods of Assessment	Methods of assessment may include but not limited to: 6.5. Written Test 6.6. Demonstration 6.7. Oral Questioning 6.8. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS007L4V1: Apply the Techniques of Web Services Hacking**
Nominal Hours	**25 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply the techniques of web services hacking in the workplace. It specifically includes the tasks of identifying web server vulnerabilities, analyzing web application, identifying web application threats and attack, applying session hijacking and provide sufficient logging and monitoring
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Identify Web server Vulnerabilities	1.1 Web Server Concepts is Identified;
	1.2 Web Server concept is interpreted;
	1.3 Web Server Package in systems is Installed;
	1.4 Vulnerabilities of **web service** is Identified using SOP;

2. Analyze web application	2.1 Web application and services are Identified; 2.2 Scanned for vulnerabilities in Web application using SOP; 2.3 Vulnerabilities of web service is analyzed using SOP;
3. Identify Web Application and service Threats & Attack	3.1 Web application for Vulnerability scanning and Automated security scanning are scanned using SOP; 3.2 Use **hacking tools** for threats and **attacks;**

4. Apply Session Hijacking	4.1 Session hijacking Concepts is interpreted;
	4.2 **Session hijacking Tools** is identified;
	4.3 Stealing is performed using session Hijacking Tools;
	4.4 Attacks are interpreted;
	4.5 Ethical Attacks are performed;

5. Provide sufficient logging and monitoring	5.1 Events are unlogged, e.g., failed logins or high-value transactions; 5.2 Back up of logs are avoided (intruders that access a system will often delete logs to obscure their movements so you won't be able to backtrack to the source of the intrusion); 5.3 Software misconfigurations are avoided that fail to alert on apparently unimportant events, e.g., a failed login or a seemingly innocuous read-only event; 5.4 Obscure error logging are ensured without enough details for forensics to follow up on or for administrators to understand the problem; 5.5 Lack of a formal escalation plan are avoided that following a breach; 5.6 Presence of automated auditing and monitoring security frameworks are ensured;

	5.7 Skilled security personnel are used to analyze log data; 5.8 Reliable authentication management is needed; 5.9 Sufficient logging and monitoring training are provided;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. web service	1.1 IIS, 1.2 Apache 1.3 Nginx, 1.4 JSON 1.5 REST
2. Hacking tools	2.1 Zed Attack Proxi (ZAP), 2.2 WFUZZ 2.3 Wapiti 2.4 W3af 2.5 SQL Map 2.6 Arachni 2.7 BurpSuite 2.8 Netsparker,
3. Session hijacking tools	3.1 Bettercap 3.2 Nettoolkit 3.3 Cookiecatcher 3.4 Firesheep 3.5 Hamster 3.6 Sslstrip 3.7 Jhijack 3.8 SQLmap
4. Attacks	4.1 Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc) 4.2 Practice Man-in-the-middle attack 4.3 Define Man-in-the-browser attack 4.4 Define meet-in-the-middle attack
Evidence Guide The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency	
1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Installed Web Server Package in systems 1.2 Used hacking tools for threats and attacks 1.3 Performed Ethical Attacks 1.4 Provided sufficient logging and monitoring;
2. Underpinning Knowledge	2.1. Web Server 2.2. Web service 2.3. Session hijacking 2.4. Ethical Attacks 2.5. Authentication management

3. Underpinning Skills	3.1 Identifying web server 3.2 Identifying web service 3.3 Applying concept of hijacking
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS009L5V1: Apply Vulnerability Assessment**
Nominal Hours	**60 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply vulnerability assessment in the workplace. It specifically includes the tasks of interpreting vulnerability concept, interpreting the concept of database system, retrieving Data using the SQL, applying SQL Functions and DML to Manipulate Data, using vulnerability assessment tools and preparing VA report.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret vulnerability concept	1.1 **Vulnerability assessment** is interpreted;
	1.2 Vulnerability assessment in Cyber Security is comprehended;
	1.3 Types of vulnerability assessment are identified;

2. Interpret the concept of database system	2.1 Database Management System (DBMS) is explained;
	2.2 DBMS & RDBMS are compared;
	2.3 Architecture of DBMS are interpreted;
	2.4 **Relational Operators, Relational Algebra Operators** and **Relational Set Operator** are explained;

3. Retrieve Data Using the SQL	3.1. SQL Language is defined;
	3.2. Basic Select Statement are executed;
	3.3. Structured Query Language (SQL) are applied to design, develop, deploy of database;

4. Apply SQL Functions and DML to Manipulate Data	4.1 **Single Row Function** handling are applied for manipulate data; 4.2 **Multiple Row Function** are applied for handling data; 4.3 Insert, Update and Delete Statement are applied for manipulating the data;
5. Use Vulnerability Assessment tools	5.1 **Vulnerability Assessment tools** are identified as per requirement; 5.2 Vulnerability Assessment tools are installed; 5.3 Vulnerability Assessment tools are updated and upgraded with dependency;
6. Prepare VA Report	6.1 Risks and Vulnerabilities using recommended tools are analyzed; 6.2 Vulnerability Assessment report is prepared following standard framework; 6.3 Vulnerability Assessment report is submitted to the controlling authority;
Range of Variables	
Variable	**Range** (may include but not limited to):

1. Vulnerability Assessment	1.1 Network Vulnerabilities 1.2 OS Vulnerabilities 1.3 Human Vulnerabilities 1.4 Process Vulnerabilities 1.5 Database Vulnerabilities
2. Relational Operators	2.1 > greater than 2.2 < less than 2.3 >= greater than or equal to 2.4 <= less than or equal to 2.5 <> not equal to 2.6 = equal
3. Relational Algebra Operators	3.1 Brackets or parentheses 3.2 Division 3.3 Multiplication 3.4 Subtraction 3.5 Addition
4. Relational Set Operator	4.1 Union 4.2 Intersect 4.3 Join
5. Single Row Function	5.1 Numeric Function 5.2 Date Function 5.3 Character Function
6. Multiple Row Function	6.1 Aggregate functions 6.2 Sum, Avg, Count, max, min, variance, studded, etc 6.3 Group by clause 6.4 Having Clause 6.5 Group by and Having functions
7. Vulnerability Assessment Tools	7.1 BurpSuite 7.2 OWASP ZAP 7.3 Netsparker 7.4 Accunetix 7.5 Varracuda 7.6 Wireshark 7.7 MBSA 7.8 Mozilla observatory 7.9 Sn1per

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Interpreted DBM and RDBM 1.2 Identified types of vulnerability assessment; 1.3 Installed vulnerability assessment tools; 1.4 Prepared vulnerability assessment report;
2. Underpinning Knowledge	2.1 DBM 2.2 RDBM 2.3 Cyber security 2.4 Risk and Threats 2.5 Assessment

	2.6 Countermeasures
3. Underpinning Skills	3.1 Applying concept of DBM and RDBM 3.2 Applying concept of vulnerabilities 3.3 Applying concept of assessment tools
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS008L4V1: Apply Information Security Systems Bypass**
Nominal Hours	**20 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply information security systems bypass. It specifically includes the tasks of interpreting information security systems bypass, analyzing security solutions to identify vulnerabilities and using tools to bypass the security solutions.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret Information Security Systems Bypass	1.1 CIA Triad is interpreted;
	1.2 Method of information Systems Security Bypass is interpreted;
	1.3 **Security solutions** is interpreted;

2. Analyze Security Solutions to identify Vulnerabilities	2.1 Types of Security Systems Assessment Tools is identified; 2.2 Vulnerabilities of Information Systems are analyzed using required tools;
3. Use Tools to Bypass the Security Solutions	3.1 **Tools** are identified as per job requirement; 3.2 Security solutions are Bypassed;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Security solutions	a. Fire wall b. IPS c. IDS d. Honeypot
2. Tools	2.1 Netsparker 2.2 W3AF 2.3 Snort 2.4 BLP 2.5 WAF Bypass 2.6 John the Ripper 2.7 Nmap 2.8 OpenVAS 2.9 Aircrack-ng 2.10 Nikto 2.11 SQL Ninja 2.12 Script Base 2.13 CryptExe 2.14 Exeref 2.15 Chimera.
Evidence Guide The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency	

1. Critical Aspects of Competency	Assessment required evidence that the candidate:
	1.1 Identified types of Security Systems Assessment Tools
	1.2 Analyzed Vulnerabilities of Information Systems;
	1.3 Bypassed security solutions;

2. Underpinning Knowledge	2.1. CIA Triad 2.2. Information Systems Security Bypass 2.3. Bypass Security solutions
3. Underpinning Skills	3.1 Applying concepts of Systems Security Bypass 3.2 Applying concepts of Systems Security Tools
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA *certified assessor*

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Copyright

This Competency Standard for **Penetration Testing (Cyber Security)** is a document for the development of curricula, teaching and learning materials, and assessment tools. It also serves as the document for providing training consistent with the requirements of industry in order for individuals who graduated through the established standard via competency-based assessment to be suitably qualified for a relevant job.

This document is owned by the National Skills Development Authority (NSDA) of the People's Republic of Bangladesh, developed in association with **ICT Industry Skills Council (ISC)**.

Public and private institutions may use the information contained in this standard for activities benefitting Bangladesh.

Other interested parties must obtain permission from the owner of this document for reproduction of information in any manner, in whole or in part, of this Competency Standard, in English or other language.

This document is available from:

National Skills Development Authority (NSDA)
423-428 Tejgaon Industrial Area, Dhaka-1215
Phone: +880 2 8891091; Fax: +880 2 8891092; E-mail: ecnsda@nsda.gov.bd
Website: www.nsda.gov.bd