GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)

Competency-focused Outcome-based Green Curriculum-2021 (COGC-2021)
Semester-II

Course Title: Information Security Awareness
(Course Code: 4321603)

Diploma programme in which this course is offered	Semester in which offered
Information Technology	Second

1. RATIONALE

As digital services are increasing, so are security attacks. Almost all successful information security breaches have one variable in common: human error. The technological advancement in terms of security has become very effective but the effectiveness of technical security measures only goes as far as humans properly utilize them. In today's digital world, information security is more important than ever. It is no longer the responsibility of security professionals only; Individuals are equally responsible too.

Cyber-attacks and cybercrimes have increased significantly. As a result, awareness of the risks and consequences of cybercrime and cyber attacks is a critical first step in establishing a secure information society. This course is therefore so designed that the students will be able to apply the principles of information security along with the tools as and when required to mitigate the threat.

2. COMPETENCY

The purpose of this course is to help the student to attain the following industry identified competency through various teaching learning experiences:

- **Use information security concepts along with various security tools and techniques for data protection.**

3. COURSE OUTCOMES (COs)

The practical exercises, the underpinning knowledge and the relevant soft skills associated with this competency are to be developed in the student to display the following COs:

a) Explain Importance of information security awareness for data protection and attacks in system security.
b) Apply knowledge of security threats to computer systems, and perform countermeasures to secure a computer.
c) Apply various tools and techniques to secure mobile devices, email and web browsers.
d) Implement various social engineering strategies to minimize the risk of data being compromised through human error.
e) Use computing and internet resources based on legal and ethical factors to understand cybercrime and law.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme (In Hours)			Total Credits (L+T/2+P/2)	Examination Scheme				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	CA	ESE	CA	ESE	
0	1	4	3	0	0	25*	25	50

(*): Out of 25 marks under the theory CA, 10 marks are for assessment of the micro-project to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessing the attainment of the cognitive domain UOs required for the attainment of the COs.

***Legends: L**-Lecture; **T** – Tutorial/Teacher Guided Theory Practice; **P** - Practical; **C** – Credit, **CA** - Continuous Assessment; **ESE** - End Semester Examination.*

5. SUGGESTED PRACTICAL EXERCISES

The following practical outcomes (PrOs) that are the sub-components of the COs. *Some of the **PrOs** marked **'*'** are compulsory, as they are crucial for that particular CO at the 'Precision Level' of Dave's Taxonomy related to 'Psychomotor Domain'.*

Sr. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. required
1	Prepare a case study on recent 2 information security attacks. Summarize and discuss which part of the CIA triad has been broken in each.	I	02
2	Choose any 2 real-world examples of security attacks and identify techniques and tools used by attackers for active and passive attacks.	I	02
3	Install Spyrix Free Keylogger, Iwantsoft Free Keylogger, or any other keylogger. configure your PC to monitor the system for keystrokes and screenshots.	II	04
4	Protect your personal computer system by creating a secure User Accounts policy for safety and security	II	02
5	Configure windows firewall for inbound and outbound rules.	II	04
6	Use USB security software such as Autorun Deleter, Panda USB Vaccine to minimize risk from removable devices.	II	02
7	Use EaseUSTodo Backup or any other tool to create backup and restore your computer.	II	02
8	Configure the security settings of your browser.	III	02
9	Test browser security using the following tools and report your findings: Qualys BrowserCheck, Cloudflare ESNI Checker, Privacy Analyzer, Panopticlick, AmIUnique	III	04
10	Test your email data breach which can be used for identity theft using following tools: 1. https://www.f-secure.com/en/home/free-tools/identity-theft-checker 2. https://haveibeenpwned.com/	III	02

Sr. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. required
	If your identity is compromised then prepare a report on how to mitigate the risk?		
11	Analyze and identify normal and spam E-mail headers using any header analyzer tool for fraud or phishing emails. Summarize your finding in the report. (Tool: https://mailheader.org/ or any other)	III	04
12	Secure your mobile device 1. Prevent installation of third-party applications. 2. Check permissions given to the installed application and evaluate whether the given permission is actually required by that application i.e., message application should not have permission to access camera 3. To prevent your device from connecting to poorly configured or insecure networks disable auto-connect in wifi settings. 4. Turn off location services, Bluetooth, wifi, mobile data as and when it is not required 5. Configure backup and restore data settings on your mobile device	III	02
13	Use Google password manager available at given link https://passwords.google.com/ to save, manage, protect and create strong passwords.	III	02
14	Demonstrate a phishing attack simulation with the GoPhish tool.	IV	04
15	Test website authenticity and possible phishing websites using VirusTotal, Google Transparency Report, URLVoid, or any other tools. Identify ways to report Fraudulent or Scam Websites.	IV	04
16	Configure all privacy settings for social networks with which you have an account and review your entire profile.	IV	04
17	Survey recent social media scams like lottery scams, job scams and prepare a report for the following: ● What is the attacker trying to gain? ● Who is being scammed? ● What are the consequences for the person being scammed? ● Why does the scam work successfully? ● What awareness is required which could avoid the scam?	IV	04
18	Study a government Cybercrime portal to prepare a report on cybercrime and its laws.	V	02
19	Prepare a report on how to report cybercrime online	V	02
20	Prepare a report on online acceptable behavior against unethical behavior.	V	02
	Total		**56**

Note

i. *More **Practical Exercises** can be designed and offered by the respective course teacher to develop the industry relevant skills/outcomes to match the COs. The above table is only a suggestive list.*

*i. The following are some **sample** 'Process' and 'Product' related skills (more may be added/deleted depending on the course) that occur in the above listed **Practical Exercises** of this course required which are embedded in the COs and ultimately the competency..*

Sr. No.	Sample Performance Indicators for the PrOs	Weightage in %
1	Analyze and identify a suitable approach for problem-solving	25
2	Use of appropriate technology/software/tools	25
3	Relevance and quality of output	20
4	Interpret the result and conclusion	15
5	Prepare a report/presentation for the given problem	15
Total		**100**

6. MAJOR EQUIPMENT/ INSTRUMENTS REQUIRED

These major equipment with broad specifications for the PrOs is a guide to procure them by the administrators to usher in uniformity of practicals in all institutions across the state.

Sr. No.	Equipment Name with Broad Specifications	PrO. No.
1	Computer system with an operating system and Internet Facility	All
2	Spyrix Free Keylogger, Iwantsoft Free Keylogger	3
3	Autorun Deleter, Panda USB Vaccine	6
4	EaseUSTodo Backup	7
5	GophishOpen-Source Tool	14

7. AFFECTIVE DOMAIN OUTCOMES

The following ***sample*** Affective Domain Outcomes (ADOs) are embedded in many of the above mentioned COs and PrOs. More could be added to fulfil the development of this competency.

a) Work as a leader/a team member.
b) Follow ethical practices.

The ADOs are best developed through the laboratory/field based exercises. Moreover, the level of achievement of the ADOs according to Krathwohl's 'Affective Domain Taxonomy' should gradually increase as planned below:

i. 'Valuing Level' in 1st year
ii. 'Organization Level' in 2nd year.
iii. 'Characterization Level' in 3rd year.

9. UNDERPINNING THEORY

Only the major Underpinning Theory is formulated as higher level UOs of *Revised Bloom's taxonomy* in order development of the COs and competency is not missed out by the students and teachers. If required, more such higher level UOs could be included by the course teacher to focus on attainment of COs and competency.

Unit	Unit Outcomes (UOs) (4 to 6 UOs at Application and above level)	Topics and Sub-topics
Unit – I Basics of Information security and awareness	1a.Explain fundamentals of security aspects 1b. Explain Security principles 1c. Understand the threats and risks to modern data and information systems. 1d.Differentiate between active and passive security attacks	1.1 What is Information Security, Importance of Information Security and its awareness 1.2 CIA Triad, Parkerian Hexad 1.3 Information security threats 1.4 Security attacks- active and passive
Unit – II Computer System Security	2a. Justify the need for operating system security 2b. Identify the risks associated with the usage of removable devices and drives 2c. Manage secure user accounts to access the operating system 2d. Apply operating system hardening techniques 2e. Apply configuration of the firewall for operating system security 2f. Differentiate between the types of malwares and their effects	2.1 Function of Operating system, importance of Operating System security 2.2 Removable Devices & Drives: Introduction, Types, Risks involved while using the removable devices, Best Practices for safe & secure usage. 2.3 Secure User Account Policy 2.4 Operating system Hardening - strong passwords, OS updates, software patches, system back-ups, Installing and Updating Antivirus, 2.5 Configuration of a firewall for OS security 2.6 Malware, Ransomware & Key-loggers: Introduction and types of malwares (Virus, Worms, Trojans, Rootkits, Adware, Spyware, Crimeware)
Unit-III Mobile Devices, Email and Web browser Security	3a. Describe Mobile Security 3b. Classify mobile deceive threats into broad categories. 3c. Identify security measures to prevent the mobile threat 3d. Analyze ways to prevent attacks on passwords.	3.1 Introduction to Mobile Security 3.2 Types of threats on mobile devices: application-based, web-based, network and physical threat 3.3 Security measures to prevent the mobile threat, Secure data on a lost mobile device 3.4 Importance of password, common Attacks on Password, Password Best Practices, maintaining good

Unit	Unit Outcomes (UOs) (4 to 6 UOs at Application and above level)	Topics and Sub-topics
	3e. Infer methods to maintain good password 3f. Survey mobile device protection methods 3g. Assess email security concepts to use email safely 3h. Analyze web security features and risks to improve web browser security	password, Multi-Factor Authentication (MFA), Password Manager 3.5 Mobile device protection: device hardening, managing app permissions, secure WI-FI, screen locks, downloading and updating Apps, backup 3.6 Email Security: How an E-mail Works, Threats through Emails, Guidelines for using Email Safely 3.7 Web Browser Security: Web Browser feature and risks, how to improve web browsers security, Security Extensions in Browsers, content filtering
Unit– IV Social Engineering and Social Networking Security	4a. Demonstrate knowledge of Internet safety practices and policies to protect one on social networks. 4b. Describe risks associated with social networks 4c. Compare similarities and differences between offline and online scams. 4d. Explain why social engineering is an important consideration for cyber security. 4e. Analyze how particular social engineering attacks take advantage of specific features of the Internet and of human nature.	4.1 Introduction to Social Network, safe and proper use of Social Network, flagging and reporting of inappropriate content on Social Network 4.2 Frauds and harassment on social media through fake profiles, sextortion using video call, cyberstalking, Cyberbullying 4.3 Spotting fake news, fake posts, fake messages, fake customer care/toll-free numbers on social media 4.4 What is social engineering? 4.5 Types of Social engineering attacks - Phishing, Spear Phishing, Smishing, Vishing, Pretexting, Search Engine Phishing Attack, Whaling, scareware, baiting, Quid Pro Quo 4.6 Ways to prevent social engineering attacks
Unit– V Cyber Crimes and Internet ethics	5a. Classify cybercrimes from the nature of the crime. 5b. Describe laws relevant to cybercrime 5c. Summarize methods to report	5.1 What is cybercrime, Categories of Cyber Crimes, Cyber Crime laws 5.2 Cyber Crime Reporting: How to Report Cyber Crimes? Report & Track Cyber Crime Complaints

Unit	Unit Outcomes (UOs) (4 to 6 UOs at Application and above level)	Topics and Sub-topics
	cybercrime and track cybercrime 5d. Distinguish ethical behavior with unethical behavior	5.3 Internet Ethics: Introduction Internet Ethics, Unethical behavior in Internet & Examples, Acceptable behavior and Examples

***Note**: The UOs need to be formulated at the 'Application Level' and above of Revised Bloom's Taxonomy' to accelerate the attainment of the COs and the competency.*

10. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Basics of Information security and awareness	04	---Not Applicable---			
II	Computer System Security	14				
III	Mobile Devices, Email and Web browser Security	16				
IV	Social Engineering and Social Networking Security	16				
V	Cyber Crimes and Internet ethics	06				
Total		**56**				

***Legends:** R=Remember, U=Understand, A=Apply and above (Revised Bloom's taxonomy)*

***Note**: This specification table provides general guidelines to assist student for their learning and to teachers to teach and question paper designers/setters to formulate test items/questions assess the attainment of the UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary slightly from above table.*

11. SUGGESTED STUDENT ACTIVITIES

Other than the classroom and laboratory learning, following are the suggested student-related ***co-curricular*** activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct following activities in group and prepare reports of about 5 pages for each activity, also collect/record physical evidences for their (student's) portfolio which will be useful for their placement interviews:

a) Register on https://cybercrime.gov.in/Webform/CyberVolunteerinstruction.aspx as a "Cyber Volunteer" to serve society in making cyberspace clean and safe.
b) Make online safety infographics, posters, or cartoons that contain cyber safety tips and circulate them within your social media to alert other users.

c) Play security awareness games on the following link or any other similar website with your friends and family members: https://www.cdse.edu/Training/Security-Awareness-Games/?utm_source=pocket_mylist
d) Study different cybercrime cases and their verdict on following or any other site: https://www.cyberlawsindia.net/cases.html
e) Undertake course on https://onlinecourses.swayam2.ac.in/nou22_cs04/preview or any other site

12. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

These are sample strategies, which the teacher can use to accelerate the attainment of the various outcomes in this course:

a) Massive open online courses (***MOOCs***) may be used to teach various topics/sub topics.
b) Guide student(s) in undertaking micro-projects.
c) ***'L' in section No. 4***means different types of teaching methods that are to be employed by teachers to develop the outcomes.
d) About ***20% of the topics/sub-topics*** which are relatively simpler or descriptive in nature is to be given to the students for ***self-learning***, but to be assessed using different assessment methods.
e) With respect to ***section No.11***, teachers need to ensure to create opportunities and provisions for ***co-curricular activities***.

13. SUGGESTED MICRO-PROJECTS

Only one micro-project is planned to be undertaken by a student that needs to be assigned to him/her in the beginning of the semester. In the first four semesters, the micro-project are group-based. However, in the fifth and sixth semesters, it should be preferably be ***individually*** undertaken to build up the skill and confidence in every student to become problem solver so that s/he contributes to the projects of the industry. In special situations where groups have to be formed for micro-projects, the number of students in the group should ***not exceed three.***

The micro-project could be industry application based, internet-based, workshop-based, laboratory-based or field-based. Each micro-project should encompass two or more COs which are in fact, an integration of PrOs, UOs and ADOs. Each student will have to maintain a dated work diary consisting of individual contributions in the project work and give a seminar presentation of it before submission. The total duration of the micro-project should not be less than ***16 (sixteen) student engagement hours*** during the course. The student ought to submit a micro-project by the end of the semester to develop the industry orientedCOs.

A suggestive list of micro-projects is given here. This has to match the competency and the COs. Similar micro-projects could be added by the concerned course teacher:

a) Use privacy-protected search engines for internet searching and compare their results with normal search engines.
b) Use private browsers and compare results with normal browsers in terms of tracking.
c) Search for your pictures on reverse image search engines and Track where and how your images appear online.
d) Create a password strength checker using python

14. SUGGESTED LEARNING RESOURCES

Sr. No.	Title of Book	Author	Publication with place, year and ISBN
1	Cyber Security	Nina Godbole, SunitBelapure	Wiley Publication ISBN: 9788126521791
2	Cryptography and Network Security - Principles and Practice | Seventh Edition	William Stallings	Pearson Education; Seventh edition (30 June 2017) ISBN: 978-9332585225
3	Cryptography And Network Security | 3rd Edition	Forouzan Behrouz, Debdeep Mukhopadhyay	McGraw Hill Education ISBN: 978-9339220945
4	Information Security-Principles and Practices	Mark Merkow	Pearson Education.ISBN- 978-81-317-1288-7

15. SOFTWARE/LEARNING WEBSITES

a) https://infosecawareness.in/
b) http://www.isea.gov.in/
c) https://www.csk.gov.in/security-tools.html
d) https://www.cert-in.org.in/
e) https://thehackernews.com/
f) https://www.infosecurity-magazine.com/
g) https://threatpost.com/
h) https://cybercrime.gov.in/

16. PO-COMPETENCY-CO MAPPING

Semester II	Information Security Awareness (4321603)									
	POs and PSOs									
Competency & Course Outcomes	**PO 1** Basic & Discipline specific knowledge	**PO 2** Problem Analysis	**PO 3** Design/ development of solutions	**PO 4** Engineering Tools, Experimentation &Testing	**PO 5** Engineering practices for society, sustainability & environment	**PO 6** Project Management	**PO 7** Life-long learning	**PSO 1**	**PSO 2**	**PSO 3** (If needed)
Competency *Use principles of basic electronics in various engineering applications*										
Course Outcomes CO a) Explain Importance of information security awareness for data protection and attacks in system security.	3	-	-	1	1	1	2			
CO b) Apply knowledge of security threats to computer systems, and perform countermeasures to secure a computer.	1	2	-	3	2	1	2			
CO c) Apply various tools and techniques to secure mobile devices, email, and web browser	1	2	1	3	2	1	2			
CO d) Implement various social engineering strategies to minimize the risk of data being compromised through human error.	2	2	1	3	2	1	2			
CO e) Use computing and internet resources based on legal and ethical factors to understand cybercrime and laws.	1	-	-	3	2	1	2			

Legend: '**3'** for high, '**2**' for medium, **'1'** for low or **'-'** for the relevant correlation of each competency, CO, with PO/ PSO

17. COURSE CURRICULUM DEVELOPMENT COMMITTEE

GTU Resource Persons

Sr. No.	Name and Designation	Institute	Email
1	Prof. Manoj Parmar	HOD-IT RCTI,Ahmedabad	manojec@gmail.com
2	Mr. Saifee Vohra	Government Polytechnic, Ahmadabad	saifeevohra@gmail.com
3	Dr. Lataben J.Gadhavi	Government Polytechnic, Gandhinagar	latagpg@gmail.com
4	Mrs.Hemali L. Vithalani	Government polytechnic for Girls, Ahmadabad	vithalani.hemali@gmail.com