IS376 Human Factors and Information Security Engineering					
Credit Hours:	3-0-3	**Prerequisites**	IS201		
Course Learning Outcomes:					
S No	**CLO**		**Domain**	**Taxonomy Level**	**PLO**
1.	Comprehend human factors requirements of socio-technical systems and the need to maintain business continuity whilst balancing long term information security		Cognitive	2	1
2.	Analyze the links between behavioral economics and human factors and maintaining a culture of information security awareness in the organization		Cognitive	4	2
3.	Develop and justify innovative solutions to promoting and managing the human factor element of information security to provide workable and effective security whilst balancing risks, costs, benefits and protection		Cognitive	3	4
Course Content:					
Understanding human performance characteristics and limitations, and the various research, design, and evaluation methods needed to address them when engineering secure systems. Perception, cognition, memory, situation awareness, decision making, stress, automation, and human-computer display and interaction design principles. Human Factors: Soft systems, human factors integration (HFI), training, trust, organizational learning, information and knowledge management. Cyber Psychology: Explore the impact of the internet and social media applications on individuals, groups, organizations and society, and human factors relevant to cyber security and online behaviors.					
Teaching Methodology:					
Lectures, Written Assignments, Semester Project, Presentations					
Course Assessment:					
Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam					
Reference Materials:					
1. David Lacey. Managing the Human Factor in Information Security: How to win over staff and influence business managers, 2009 2. Angeline Prasanna Gopalan. A Novel Authentication Using Multimodal Biometrics System, November 2019 In addition there will be lecture notes and selected articles.					