PG Diploma in IT Infrastructure, Systems and Security (PG-DITISS)

The theoretical and practical mix of the Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) programme has the following focus:

- To understand the Concepts of Data Centre Management, applications security implementation and use various techniques for Ethical Hacking and Cyber Forensics
- To analyze the Threats Detection Techniques, Intrusion Detection and Prevention measures
- To use advanced tools/ decision-making tools/ techniques to analyze the complex problems and get ready to develop such new techniques for the future
- To learn cloud computing, accessing resources and services needed to perform functions with dynamically changing needs thereby implementing cloud privacy and security concepts on cloud platforms to create secure cloud environment
- To analyze and solve problems conceptually and practically from diverse industries, such as government manufacturing, retail, education, banking/ finance, healthcare and pharmaceutical
- To undertake industrial research projects for the development of future solutions in the domain of Information Security to make an impact in the technological advancement

Detailed Course Content:

1. **Fundamental of Computer Networks:** Introduction to communication system, Overview of Transmission Media, OSI Layers, TCP/IP Models, Router IOS & Security Device Manager, Managing an Internetworking Router, Overview of LAN (local area networks), VLAN (virtual local area network), Configuration of switch, Overview of STP, Discussion of Networking Protocols, IP Addressing (Fixed Length Subnet Masking, Variable Length Subnet Masking, Classless Inter Domain Routing), Static Routing and Dynamic Routing (RIP, IGRP, EIGRP, OSPF), Introduction to NAT, Introduction to IPv6, Introduction of WAN, Infrastructure Security, Software defined network
2. **Concepts of Operating System and Administration**:
    a. Concepts of OS: Architecture of Operating System, Process Management, Memory Management, File system Management, Network Operating System
    b. Windows Operating System and Security Issue: Overview of windows operating system, Overview of Administrative Tasks and Tools, Installation of windows operating system, Windows 10/ server 2016 core, Deploying Windows with WDS, Network Configuring, Implementation of infrastructure of windows networks, File system and disk management, Registry settings, System Configuration Settings, Configuration of IIS SQL server, web server and Exchange server, Implementing and administering Active Directory, User accounts and groups in an Active Directory Domain, Maintenance and troubleshooting, Microsoft Windows os Licensing model, Power shell Scripting, Windows Administration using power shell, Background Jobs and Remote Administration.
    c. Linux Operating System and Security Issue: Systems Concepts, Startup Files, Linux boot process, Installation of Linux, Basic linux commands, Configuring the GRUB boot loader, Disk partition, Controlling and managing Services, Repository configuration, User administration of Linux, Network Configuring, Network Teaming/Load balancing, Define network

route, Using SSH for network communications, Using VNC for remote management, Network Authentication, Patches & updates, System Configuration Files, Perform System Management, X configuration server, Package management, The Samba Server, Configuring a DHCP server, Configuring a DNS server, Configuring the Apache web server, Maintenance and troubleshooting, SE LINUX/ APParmor, Basic Service Security, Log Management and NTP, BIND and DNS Security, Network Authentication: RPC, NIS and Kerberos, Apache security(SSL), Bash Scripting, Introduction to BASH Command Line Interface (CLI) Error Handling Debugging & Redirection of scripts, Control Structure, Loop, Variable & String Conditional Statement, Regular Expressions, Automate Task Using Bash Script, Security patches, Logging & Monitoring using script.

3. Security Concepts:

a. MySQL: Introduction to MYSQL, Installing and Configuring MYSQL, Creating and Dropping Database, Queries in MYSQL, Web Application Security Risks, Identifying the Application Security Risks, Threat Risk Modelling, Other HTTP fields, Data Extraction, Advanced Identification/Exploitation

b. Web Application Security: OWASP Top 10 –2017, Injection and Inclusion, Cross Site Scripting, Injection in stored procedures, Denial of Service, Buffer Overflows and Input Validation, Access Control, DevOps Security, API Security, OWASP top 10 Cloud security Risks, Secure CodeReview, SAST and DAST tools, Case Study on Web Application Framework, use browser-jsguard Firefox add-on also to detect Malicious and Suspicious Webpages.

c. Mobile Security: Introduction to Android Architecture, Android File Structure, Android Build Process, Android App fundamentals, Android Security Model, Device Rooting, Android Debug bridge, Penetration Testing Tools, OWASP Top 10 Mobile App vulnerabilities, Attacks on Android Apps, Web based attacks on Android devices, Networks based attacks, Social Engineering attacks, Overview of Mobile Malware, Android App Analysis

d. Python: Introduction to Python, Python basics, Data Types and variables Operators, Looping & Control Structure List, Modules Dictionaries, string Regular Expressions, Functions and Functional Programming, Object Oriented Linux Scripting Environment, Classes, Objects and OOPS concepts, File and Directory Access Permissions and Controls Socket, Libraries and Functionality Programming, Servers and Clients Web Servers and Client scripting, Exploit Development techniques. Writing plugins in Python, Exploit analysis Automation Process, Debugging basics, Task Automation with Python

e. Ethical Hacking: Introduction to Ethical Hacking, Understanding Ethical Hacking Terminology, Identifying Different Types of Hacking Technologies, Understanding the Different Phase Involved in Ethical Hacking, Types of Hacker Classes, Ethical Hackers and Crackers, Goals of Attackers, Security, Functionality and Ease of Use Triangle, Ethical Hacking procedure, Creating a Security Evaluation Plan, Foot-printing and Social Engineering, Tracerouting, Port Scanning, Network Scanning and Vulnerability Scanning, SYN, Stealth, XMAS, NULL, IDLE and FIN Scans, TCP Communication Flag Types, Banner Grabbing and OS Finger printing Techniques, Using Proxy servers in launching an Attack, Http tunneling Techniques, IP Spoofing Techniques, Enumeration, Password-cracking Techniques, Cracking Windows Passwords, Redirecting the SMB Logon to the attackers, SMB

Redirection, SMB Relay MITM Attacks and Countermeasures, NetBIOS DOS Attacks, DDos Attack, Password-Cracking Countermeasures, Active/Passive online Attacks, Offline Attacks, Keyloggers and other Spyware Technologies, Trojans and Backdoors, Overt and Covert Channels, Types of Trojans, Reverse-connecting Trojans, Netcat Trojan, Indications of a Trojan Attacks, Wrapping, Trojan Construction Kit and Trojan Makers, The countermeasure Techniques in Preventing Trojans, Trojan Evading techniques, System File Verification, Virus and a Worm, Antivirus Evasion Techniques, Virus Detection Methods, Protocols Susceptible to Sniffing, Active and Passive Sniffing, ARP Poisoning, Ethereal Capture and Display Filters, MAC Flooding, DNS Spoofing Techniques, Sniffing Countermeasures, Types of DOS Attacks, Smurf Attacks, SYN Flooding, Spoofing vs Hijacking, Types of Session Hijacking, Steps to perform session Hijacking, Prevention of session Hijacking, Hacking WebServers, Web Application Vulnerabilities, Web-Based Password Cracking Techniques, Wireless Hacking, WEP, WPA Authentication Mechanisms and Cracking Techniques, Wireless Sniffers and Locating SSIDS, Wireless hacking Techniques, Methods used to secure Wireless Networks, IDSs, Honeypots and Firewalls.

4. **Compliance Audit:** What Cybersecurity Challenges do Organizations Face?, Compliance and Regulations for Cybersecurity ,Compliance Basics, Compliance Frameworks and Industry Standards, National Institute of Standards and Technology (NIST) , General Data Protection Regulation (GDPR) , International Organization for Standardization (ISO) 2700x, SOC Reports, SOC Reports - Auditor Process Overview, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS),COBIT Framework, Center for Internet Security (CIS) Critical Security Controls.
5. **Network Defense and Countermeasures (NDC):** Security Fundamentals, Firewalls, Types of Firewalls, Overview of NextGen Firewall, Limitations of firewall, Intrusion Detection and Prevention, Intrusion risks, Security policy, Monitoring and reporting of traffics, Traffic shaping, Investigating and verifying detected intrusions, recovering from, reporting and documenting intrusions, Define the Types of intrusion Prevention Systems, Intrusion prevention system basics, Limitations of Intrusion Prevention System, Spoofing Detection &Prevention, DDos & Dos mitigation techniques, Qos Policy, Introduction of Web Application Firewall, Packet Signature and Analysis, Virtual Private Networks, Deploy and managing VPN, VPN Performance tuning and error handling, DMZ and virtual host, Introduction of Reverse proxy and policies
6. **Cyber Forensics:** Introduction to Cyber Crime and Cyber Forensics, Basic Forensic Principles, Computer Forensics, Types of Cyber Forensics Techniques, Cyber Forensics Procedures, Detecting Incidents, Handling Evidence, Encoding and Encryption, Cyber Forensics Tools: Sysinternals Suite, FTK Forensics Tool kit, FTK Imager, OSF, Hex, Cyber check Suite
7. **Public Key Infrastructure:** Understand Basic Encryption Concepts, File Encryption, Encryption Folders (Graphical/ using cipher), Cryptographic Fundamentals, Cryptographic Ciphers (Symmetric and Asymmetric), Protocols (History, Usage, Key generation, Ciphering message), Symmetric Key Encryption (DES, AES, RC5), Asymmetric Key Encryption (RSA, ECC), Diffie-Hellman Key Exchange, Attacks against encryption, Cryptographic issues, Secure Hashing Methods, SHA Secure Hash algorithm, HMAC, PKI Fundamentals, Digital Signature, Digital Certificate, CA, Trust Model, Certificate Issuance Process, Certificate Revocation (CRL, OCSP), Types and Classes of Certificate, Introduction to Aadhaar and e-Sign, Time stamping Services, Public Key Cryptography Standards, PKCS, FIPS 140-2, Strong Authentication, Single Factor and Multi-factor authentication, Single Sign-on Solutions, Open-ID and OAUTH, Graphical Passwords, Authentication Protocols,

FIDO Authentication, Zero Trust Architecture, Securing Websites and Emails, SSL, TLS, PGP and S/MIME

8. **IT Infrastructure Management & DevOps**:
    a. Introduction to ITIL: Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement
    b. Data Center Management: Introduction to DCM, Data Center design, Data Center Security Procedure, Server Security, Storage area network, Virtualization, Docker, kubernets, Introduction of Virtual Private Cloud (VPC), Private Cloud Setup, Automation Using Cloud API, Server Orchestration, Cloud Logging and monitoring.
    c. DevOps: Introduction to DevOps, Docker, Kubernets, Dockerswam, Container, CI/CD Pipelines, Version Control system, containerization with Docker, MicroService Deployment.
9. **Aptitude & Effective Communication:** Fundamentals of Communication, The Art of Communication, Personality Development, English Grammar, Correct Usage of English, Common Mistakes in English Communication, Listening Skills, Reading Skills, Writing Skills, Public Speaking, Presentation Skills, Group Discussions, Interpersonal Skills, Personal Interviews
10. **Project**