e-Tender

For Public Private Partnership on Concession Based Model as Knowledge partners

Shaheed Sukhdev College
of Business Studies,
University of Delhi

Checklist for Bid Submission

(The following check-list must be filled in and submitted with the bid documents)

Sr No.	Particulars	Yes/No
1	Uploaded scanned copy of bank transfer (i.e. UTR Number) for EMD	
2	Uploaded Tender Acceptance Letter as per *Annexure-II*	
3	Uploaded Prequalification Documents as per *Annexure-III*	
4	Uploaded compliance sheet for specification as per *Annexure-V*	
5	Uploaded details of Supply, Turnover & Profit as per *Annexure-IX*	
6	Uploaded the Undertaking for Technical Bid as per *Annexure-X*	
7	Uploaded proofs for parameters required for technical evaluation	
8	Uploaded the Financial Bid as percentage share	

Notice Inviting Tender (E-procure mode)
Shaheed Sukhdev College of Business Studies
(University of Delhi)
Delhi-110089

Principal, Shaheed Sukhdev College of Business Studies (SSCBS), PSP Area-IV, Dr. K. N. Katju Marg, Sector-16, Rohini, Delhi-110089, (University of Delhi) invites Online Tender through Two bid System (Technical Bid and Financial Bid) from companies to have Public Private Partnership on Concession based model, for running Post graduate diploma in cyber security and law course from coming session 2018-19.

Details of Items	Public Private Partnership on Concession based model as Knowledge partners with SSCBS, PSP Area-IV, Dr. K. N. Katju Marg, Sector-16, Rohini, Delhi-110089
Earnest Money Deposit (EMD) to be submitted in SSCBS	Earnest Money Deposit of Rs.2,00,000/- (Rupees Two lakh only) in the form of Account Payee Demand Draft,Fixed deposit Receipt, Banker's Cheque or Bank Guarantee from any commercial banks in favour of Principal, Shaheed Sukhdev College of Business Studies to be submitted in SSCBS or may transfer to the college Account as Bank Transfer (NEFT). College Bank details are (Account Name: Principal, S.S.C.B.S Maintenance A/c, Account Number: 35810777577, IFS Code: SBIN0011550, Bank: State Bank of India, Sector-11, Rohini). The bidder has to upload the Receipt received from the Cashier of the college while submitting bid through e-procurement. The bid security shall remain valid for a period of forty-five days beyond the final bid validity period. EMD of unsuccessful bidders will be returned to them at the earliest after expiry of the final bid validity and latest on or before the 30th day after the award of the contract.
Issue of Tender Document	The complete bid document can be downloaded from SSCBS website: www.sscbsdu.ac.in or from Central Public Procurement Portal: https://eprocure.gov.in/eprocure/app

CRITICAL DATE SHEET

Published Date	**2 July 2018 (5.30 pm)**
Bid Document Download / Sale Start Date	**2 July 2018 (5.30 pm)**
Clarification Start Date	**3 July 2018 (10.00 am)**
Clarification End Date	**5 July 2018 (04.00 pm)**
Bid Submission Start Date	**6 July 2018 (10.00 am)**
Bid Submission End Date	**23 July 2018 (12:00 NOON)**
Bid (Technical) Opening Date	**24 July 2018 (12:00 NOON)**

Administrative Officer,
SSCBS

Table of Contents

1. PART-I: BID SCOPE & REQUIREMENTS

1.1 SCOPE OF WORK

1.1.1 Public Private Partnership on Concession based model as Knowledge partners for running the course Post Graduate Diploma in Cyber Security and Law as mentioned at *Annexure-I,* at SSCBS, PSP Area-IV, Dr. K. N. Katju Marg, Sector-16, Rohini, Delhi-110089.

1.1.2 The following services need to be procured

Service for Procurement
Public Private Partnership on Concession based model as Knowledge partners for running the course Post Graduate Diploma in Cyber Security and Law as per Annexure 1

*** Services may increase or decrease as per requirement of the course as provided under Annexure 1.**

The College of Business Studies shall provide the following as public partner:

a. The installation of hardware as required in the course (Annexure A) with operating system to operationalize state of the art Cyber Security and forensics lab initially with 55 systems and thereafter as increased by the College of Business Studies, University of Delhi, therein.

b. College has the facilities of cafeteria, library and Hostel for students as per rules.

1.2 ELIGIBILITY REQUIREMENTS

1.2.1 This invitation of Bids is open to all Bidders fulfilling following terms and conditions (Annexure-III):

a. Be an entity as Information Technology Risk Assessment and Digital Security Services provider.
b. Having at least five years of experience in delivery of cyber security services to corporate/Government Department.
c. Be an Empanelled Information Security Auditing Organization by the Computer Emergency Response Team –India (CERT-In)
d. Having a team of cyber security professionals with at least ten full-time OSCP certified professionals.
e. Having an average annual turnover of INR Two crore or above in the last three financial years.
f. Having experience of handling cyber security projects in Banks/Government Departments/Defense Organization/Aviation/ FMCG/E Commerce in the last three years.
g. The Bidder has not been blacklisted by any of the Universities/Government Organization (s)/Public Sector Undertaking (s) (PSUs).
h. The Bidder shall have a valid GSTIN and PAN.

1.2.4 Bidder must comply with all the above mentioned criteria as mentioned. Non-compliance of any of the criteria shall result in rejection of the bid. Self-attested scanned copies of relevant documents / certificates shall be submitted as proof in support of the claims made for each of the above mentioned criteria. The Purchaser reserves the right to verify/evaluate the claims made by the bidder independently. Any hiding/ mis-representation of facts shall result in rejection of the bid and forfeiture of Bid Security.

1.3 TECHNICAL REQUIREMENTS

1.3.1 Technical Specification for Services

1.3.1.1 The Bidder shall provide services as per technical specifications mentioned in *Annexure-I*. Bidder shall ensure that all softwares supplied are licensed.

1.3.1.2 This Partnership will be for the period of five academic years starting from the day of formal agreement between college and private partner.

2 PART-II: BID PREPARATION & SUBMISSION

2.1 BIDDING PROCESS

2.1.1 The Bidder shall submit the bids electronically, through the e-procurement portal (http://eprocure.gov.in/eprocure/app). Any document submitted through any other means will not be considered as part of the Bid except for the Originals as asked for in this tender.

2.1.2 This tender shall follow a two-stage Bidding process. A Bid shall be submitted in two parts, Technical Bid and Price Bid Presentation.

2.1.3 In the first stage, only Technical Bid will be opened online and evaluated.

2.1.4 The Bid shall be considered responsive provided it meets all the requirements under this Bid document including Technical Specifications as per *Annexure-I.*

2.1.5 Technical bid evaluation may also include presentation by the bidder explaining bidders offer.

2.1.6 Under the second stage, the Price Bid Presentation of only those Bidders, whose Bids are found responsive, shall be allowed. **Date of opening of Price Bid would be notified separately.**

2.2 INSTRUCTIONS FOR ONLINE BIDDING PROCESS

2.2.1 The bidders are required to submit soft copies of their bids electronically on the CPP Portal, using valid Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the CPP Portal, prepare their bids in accordance with the requirements and submitting their bids online on the CPP Portal.

2.2.2 More information useful for submitting online bids on the CPP Portal may be obtained at: http://eprocure.gov.in/eprocure/app.

2.2.3 REGISTRATION

2.2.3.1 Bidders are required to enroll on the e-Procurement module of the Central Public Procurement Portal (URL: http://eprocure.gov.in/eprocure/app) by clicking on the link “Online bidder Enrollment” on the CPP Portal which is free of charge.

2.2.3.2 As part of the enrolment process, the bidders will be required to choose a unique username and assign a

password for their accounts.

2.2.3.3 Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPP Portal.

2.2.3.4 Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Class II or Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify / nCode / eMudhra etc.), with their profile.

2.2.3.5 Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSC's to others which may lead to misuse.

2.2.3.6 Bidder then logs in to the site through the secured log-in by entering their user ID / password and the password of the DSC / e-Token.

2.2.4 SEARCHING FOR TENDER DOCUMENTS

2.2.4.1 There are various search options built in the CPP Portal, to facilitate bidders to search active tenders by several parameters. These parameters could include Tender ID, Organization Name, Location, Date, Value, etc. There is also an option of advanced search for tenders, wherein the bidders may combine a number of search parameters such as Organization Name, Form of Contract, Location, Date, Other keywords etc. to search for a tender published on the CPP Portal.

2.2.4.2 Once the bidders have selected the tenders they are interested in, they may download the required documents / tender schedules. These tenders can be moved to the respective 'My Tenders' folder. This would enable the CPP Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.

2.2.4.3 The bidder should make a note of the unique Tender ID assigned to each tender, in case they want to obtain any clarification / help from the Helpdesk.

2.2.5 PREPARATION OF BIDS

2.2.5.1 Bidder should take into account any corrigendum published on the tender document before submitting their bids.

2.2.5.2 Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid. **Please note the number of covers in which the bid documents have to be submitted, the number of documents -including the names and content of each of the document that need to be submitted.** Any deviations from these may lead to rejection of the bid.

2.2.5.3 Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF / XLS / RAR / DWF/JPG formats. Bid documents may be scanned with 100 dpi with black and white option which helps in reducing size of the scanned document.

2.2.5.4 To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use "My Space" or ''Other Important Documents'' area available to them to upload such documents. These documents may be directly submitted from the "My Space" area while submitting a bid, and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process.

2.2.6 SUBMISSION OF BIDS

2.2.6.1 Bidder should log into the site well in advance for bid submission so that they can upload the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.

2.2.6.2 The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document.

2.2.6.3 Earnest Money Deposit of Rs.2,00,000/- (Rupees Two lakh only)) in the form of Account Payee Demand Draft,Fixed deposit Receipt, Banker's Cheque or Bank Guarantee from any commercial banks in favour of Principal, Shaheed Sukhdev College of Business Studies to be submitted in SSCBS or may transfer to the college Account as Bank Transfer (NEFT). College Bank details are (Account Name: Principal, S.S.C.B.S Maintenance A/c, Account Number: 35810777577, IFS Code: SBIN0011550, Bank: State Bank of India, Sector-11, Rohini). The bidder has to upload the Receipt received from the Cashier of the college while submitting bid through e-procurement. EMD of unsuccessful bidders will be returned to them at the earliest after expiry of the final bid validity and latest on or before the 30th day after the award of the contract.

2.2.6.4 Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BoQ format with the tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BoQ file, open it and complete the white coloured (unprotected) cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BoQ file is found to be modified by the bidder, the bid will be rejected.

2.2.6.5 The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.

2.2.6.6 All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data. The data entered cannot be viewed by unauthorized persons until the time of bid opening. The confidentiality of the bids is maintained using the secured Socket Layer 128 bit encryption technology. Data storage encryption of sensitive fields is done. Any bid document that is uploaded to the server is subjected to symmetric encryption using a system generated symmetric key. Further this key is subjected to asymmetric encryption using buyers/bid openers public keys. Overall, the uploaded tender documents become readable only after the tender opening by the authorized bid openers.

2.2.6.7 The uploaded tender documents become readable only after the tender opening by the authorized bid openers.

2.2.6.8 Upon the successful and timely submission of bids (ie after Clicking "Freeze Bid Submission" in the portal), the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.

2.2.6.9 The bid summary has to be printed and kept as an acknowledgement of the submission of the bid. This acknowledgment may be used as an entry pass for any bid opening meetings.

2.3 BIDDING DOCUMENT

2.3.1 The Bidder is expected to examine all instructions, forms, terms and conditions prequalification and technical requirements in the bidding documents. Failure to furnish any information required in the bid shall be treated as non-responsive and may result in the rejection of the bid.

2.4 BID VALIDITY PERIOD

2.4.1 The Bid shall remain valid for a period of at least 180 days from the last date of submission of bid.

2.5 TECHNICAL BID

2.5.1 The Technical Bid shall be complete in all respects and contain all information asked for in this document.

2.5.1.1 Signed & scanned copy of Checklist for Bid Submission.

2.5.1.2 Signed & scanned copy of Tender Acceptance Form as per *Annexure-II*.

2.5.1.3 Signed & scanned copy of Bidder Information as per *Annexure-IV*.

2. 5.1.4 Signed & scanned copy of Compliance Sheet for Specifications as per

Annexure -V.

2. 5.1.5 Signed & scanned copy of List of Deviations as per *Annexure-VII*.

2. 5.1.6 Signed & scanned copy of Details of offices as per *Annexure-VIII*.

2. 5.1.7 Signed & scanned copy of Details of Turnover & Profit as per *Annexure-IX*.

2. 5.1.9 Signed & scanned copy of *Annexure-III* as well as each of the Prequalification criteria documents as per *Annexure-III*.

2. 5.1.10 EMD of Rs.2,00,000/- as per details given in the tender document

2.5.2 The following documents shall be submitted, in Original, by the Bidder before the deadline of the submission of the bid:

a. EMD

2.5.3 Self-certified copies of all the relevant documents as proof in support of various scanned documents uploaded in aforesaid *Annexures* and other claims made by the Bidder shall be submitted to the Purchaser before deadline of submission of the bids. Purchaser reserves the right to verify the submitted documents with original one.

2.6 PRICE BID

2.6.1 The Price Bid shall be complete in all respects and contain all information asked for in this document.

2.6.2 The Price bid format is provided to specify share percentage along with this tender document at http://eprocure.gov.in/eprocure/app. Bidders are advised to download this BoQ_XXXX.xls as it is and quote their offer in the permitted column and upload the same in the Price bid. Bidder shall not tamper/modify downloaded price bid template in any manner. In case if the same is found to be tempered/modified in any manner, Bid will be completely rejected and Bid Security would be forfeited and tenderer is liable to be banned from doing business with the Purchaser.

2.6.3 The Bid shall be quoted in percentage of share in application money received for the program wherein the private partner shall act as knowledge partner.

2.6.3 The share percentage shall be made after deducting taxes as per norms.

2.7 NO PRICE VARIATION

2.7.1 The quoted percentage shall remain firm throughout the validity period of the bid and no revision is permissible for any reason.

3 PART-III: BID OPENING & EVALUATION

3.1 OPENING OF BIDS

3.1.1 The Purchaser shall open the bids as per electronic bid opening procedures specified in Central Public Procurement Portal (CPPP) at the date and time specified. Bidders can also view the bid opening by logging on to the e-procurement system. Specific bid opening procedures are laid down at http://eprocure.gov.in/eprocure/app under the head "Bidders Manual Kit". The bidder will be at liberty to be present either in person or through an authorized representative at the time of opening of the Bid or they can view the bid opening event online at their remote end. Price Bids of only those Bidders shall be opened whose Technical Bid are found to be responsive.

3.1.2 The purchaser will open the bids in the presence of Bidders' representative who choose to attend at the time, date and venue as mentioned in tender document.

3.1.3 No representatives are allowed to attend the Bid Opening without the valid Bid acknowledgement slip received after submission of Bids.

3.1.4 In the event of the specified date of bid opening being declared a holiday for purchaser, the bids shall be opened at the specified time and place on the next working day.

3.2 PRELIMINARY EXAMINATION OF TECHNICAL BID

3.2.1 The Purchaser will examine the bids to determine their completeness in all respect as per the requirements of this Bid Document.

3.2.2 The purchaser may waive any minor informality or non-conformity or irregularity in a bid, which does not constitute a material deviation, provided such waiver does not prejudice to affect the relative ranking of any bidder.

3.3 EVALUATION OF TECHNICAL BIDS

3.3.1 The Purchaser shall evaluate the Technical Bid based on the documents submitted as mentioned in clause 3.4 of this Bidding document.

3.3.2 Bidders have to give presentation explaining the way in which bidders will be helping the college for running this course.

3.3.3 Purchaser reserves the right to reject the bid under any of the following circumstances:

3.3.3.1 Bid is incomplete and/or not accompanied by all required documents.

3.3.3.2 Bid is not in conformity with the terms and conditions stipulated in this document.

3.3.3.3 Specifications stipulated in *Annexure-I* are not met.

3.4 TECHNICAL EVALUATION SCORE CARD

3.4.1 The bidders who fulfill the eligibility criteria will make a presentation before the evaluation committee formed by college and evaluation committee will give marks to the bidders examining the following:

	Parameters
1	Number of Students trained in the domain of cyber security
2	Number of training hours imparted so far in the domain of Cyber Security
3	Number of MDP/FDP workshops conducted so far in the domain of Cyber Security
4	Number of Existing Knowledge Partnership (s) in the domain of Cyber Security with UGC recognised University for the purpose of training and knowledge delivery.
	Total Score

Bidders will be given marks out of 60 (maximum 15 in each of the parameter) by the committee in this evaluation. Only those bidders who obtain minimum 30 marks in technical evaluation will be considered for financial evaluation.

3.5 FINANCIAL EVALUATION

3.5.1 Financial evaluation shall be done based on percentage of share of application money received by the college for the program after deducting expenses incurred in admission procedures, worked out after considering discrepancies, if any, as mentioned in the *Annexure-VI*.

4 PART-IV: AWARD OF CONTRACT

4.1 L-1 BIDDER

4.1.1 The bidder seeking lowest percentage share in application money received for the program will be awarded contract.

4.2 LETTER OF AWARD (LoA)

4.2.1 The L-1 bidder will be considered for issuing Letter of Award (LoA) in accordance with clause 3.3 and 3.4 of this Bidding document.

4.2.2 The acceptance of the LoA shall be submitted within 7 (Seven) working days from issue of LoA, failing which the college reserves the right to cancel the LoA.

4.3 PERFORMANCE SECURITY

4.3.1 A Performance Security in form of Bank draft/ Bank guarantee from any Nationalized / Scheduled Bank of a value equal to INR 5 lakh value as indicated in the Letter of Award shall be deposited by the bidder within Ten(10) working days from issue of Letter of Award) in the form of Account Payee Demand Draft,Fixed deposit Receipt, Banker's Cheque or Bank Guarantee from any commercial banks in favour of Principal, Shaheed Sukhdev College of Business Studies to be submitted in SSCBS or may transfer to the college Account as Bank Transfer (NEFT). College Bank details are (Account Name: Principal, S.S.C.B.S Maintenance A/c, Account Number: 35810777577,

IFS Code: SBIN0011550, Bank: State Bank of India, Sector-11, Rohini).

4.3.2 The Performance Security shall be valid for period of sixty days beyond the date of completion of all the contractual obligation of the supplier. The bid security of will be refunded to successful bidder on receipt of performance security.

4.4 SIGNING OF CONTRACT

4.4.1 The successful bidder shall be required to enter into a contract with the college within Ten (10) working days from issue of the Letter of Award on submission of the Performance Security as mentioned in clause 4.3.

4.5 SUB-CONTRACTING

4.5.1 The supplier shall not assign, in whole or in part, its obligations to perform under the contract, to other firm except with the Purchaser's prior written consent.

5 PART-V: DELIVERY & PAYMENT

5.1 TERMS OF EXECUTION

5.1.1 The Supplier shall install and commission all the items mentioned in the Letter of Award within forty five days from the date of issuance of the Letter of Award. However, the college reserves the right to extend this timeline. If the timeline extended by supplier without prior consent of the College than penalty of INR 2 lakhs will be levied.

5.1.2 This Partnership will be for the period of five academic years starting from the day of formal agreement between college and private partner.

5.1.3 Performance of private partner will be audited annually on the basis of following:

i. Placement of Students enrolled for this course
ii. ii. Student feedback
iii. Project placement of students etc.
iv. Software are functional and catering the need of students.
v. Compliance of the provisions of contract as mentioned in LOA and other documents.

5.1.4 The private partner cannot repudiate the partnership before successful completion of at least three years. In case the private partner intends to repudiate the partnership before the successful completion of three years, the private partner has to pay penalty equivalent to his share of revenue earned in the years served starting from the commencement of the partnership till the date if cessation of partnership and performance security will forfeited.

5.1.5 After three years the private partner may repudiate the partnership only at the end of academic session giving three months' advance notice and performance security will be forfeited. However, the college has right to break the partnership after one year on the basis of performance auditing by competent authorities, if the services delivered are not satisfactory.

5.1.6 The partnership will be repudiated automatically if course is discontinued by the University/College.

5.1.7 The private partner shall have to setup the cyber security laboratory as per Annexure 1 within forty five days from date of start of partnership.

5.1.8 For any dispute between college and private partner decision of Governing Board of Institute of Cyber Security and Law (ICSL) for this course shall be binding on both the parties.

5.1.9 The Governing Board of ICSL may alter the eligibility criteria of visiting or guest faculty based on the performance audit report of the private partner.

5.1.10 During the partnership period if the course content is modified by the university, the private partner has to provide all the new/ revised required softwares. Further, in case of new or augmented tool is used for handling the incidents, the improved/augmented tool shall be introduced in laboratory, as and when approved by the advisory council of the course.

5.1.11 Partnership period may be extended for one more year with the consent of both the parties under same term and condition, with the approval of advisory council of the course and governing body of the college.

5.1.12 The latest version of software installed by private partner shall become the property of public partner at the end of partnership.

5.1.13 The bidder has to provide performance guarantee of INR 5 Lakh in the form of Account Payee Demand Draft,Fixed deposit Receipt, Banker's Cheque or Bank Guarantee from any commercial banks in favour of Principal, Shaheed Sukhdev College of Business Studies to be submitted in SSCBS or may transfer to the college Account as Bank Transfer (NEFT). College Bank details are (Account Name: Principal, S.S.C.B.S Maintenance A/c, Account Number: 35810777577, IFS Code: SBIN0011550, Bank: State Bank of India, Sector-11, Rohini).

5.1.14 The list of faculty for delivery of lectures shall be proposed by the partner to the ICSL and shall be determined as provided under Ordinance XX (o) of University of Delhi act 1922.

5.2 LOCATIONS TO BE COVERED

5.2.1 The delivery of services is to be done as per the address mentioned in the Letter of Award. However, the Services are to be provided, during the contract period, at SSCBS, Rohini, Delhi-110089.

5.3 DELAYS IN THE SUPPLIER'S PERFORMANCE

5.3.1 Delivery of the services and performance of the Services shall be made by the supplier in accordance with the time schedule specified in the Letter of Award. Any delay in performing the obligation by the supplier will attract liquidated damages and/or termination of contract. In case of breach of secrecy or confidentiality by the private partner, the penalty shall be decided by the competent authority depending on gravity of breach as per University rules.

5.4 ORDER CANCELLATION

5.4.1 If the Bidder fails to perform as per specifications within the stipulated time schedule or the extended date communicated by the Purchaser, if any, it will be treated as breach of contract.

5.4.2 The Purchaser reserves the right to cancel the order in the event of breach of contract.

5.4.3 The Bidder may terminate the contract in case of non-resolution of dispute through Arbitration with reference to payment by giving a notice of three months.

5.5 PAYMENT TERMS

5.5.1 No advance payment will be made against Letter of Award.

5.5.2 All payments shall be paid after deducting admissible expenses incurred in admission process and relevant taxes quarterly. The payment will be made at the end every quarter on prorate basis.

6 PART-VI: ANNEXURES

Service Deliver and Laboratory

Annexure 1

Private partner will incur cost of and provide the following:

1. The installation of all software as required in the course (Annexure A) to operationalize state of the art Cyber Security and forensics lab initially with fifty systems for fifty seats and thereafter as increased by the College of Business studies, University of Delhi, therefor.
2. E Toolkit for all the students.
3. Organize management development Programme or Faculty Development Programme (MDP/FDP) and training program.
4. Presenter's Manuals for specific classes; Updated reference books and journals to be recommended to students; subscribing national and international journals for referral E library; Subject specific toolkits.
5. Professionals for conducting Webinars and International resource person from academia/ industry (preferably on virtual platform)
6. Suggest professionals having Master's degree in Computer Science or Computer Application or B.Tech. Computer Science/Electronics and certified cyber security experts with OSCP certification from an organization of repute and having at least one year of corporate experience of handling cyber security projects for engagement as guest/ visiting faculty.
7. Research & Development know-how pertaining to cyber security training in University.
8. Industrial visit (except travelling, boarding and lodging), if any.
9. Organizing annual program or event, if any, related to cyber security along with the students of College of Business Studies, University of Delhi and sponsors.
10. Provide placement opportunities each year to students completing the PGDCSL successfully.

LABORATORY Tools I : Web Application Security

Sr. No.	Tool Name	Category	Quantity
1	Metasploit Framework Pro	Penetration Testing	2
2	Burp Suite Pro	Web VA	2
3	Acunetix Web Vulnerability Scanner	Web VAPT	2
4	Netsparker Web Vulnerability Scanner	Web VAPT	2

5	Checkmark Secure Source Code Analyzer	Secure Source Code Reviewer	1

LAB Tools II: Network VAPT Security

Sr. No.	Tool Name	Category	Quantity
1	Nessus Vulnerability Scanner	Network Scanner	2
2	Alpha Cards – External USB Wifi	Wireless Security	2
3	Raspberry Pi 3 Model B	Network Security/IoT	2
4	D-Link DIR-615 Wireless N 300 Router	Network Security	2

LAB Tools III : Cyber Forensics

Sr. No.	Tool Name	Category	Quantity
1	FTK 7.0 Toolkit	Forensic Evidence Collector	1
2	Cellebrite Mobile Forensic Toolkit (UFED) for PC	Mobile Forensic	1
3	DVR Duplicator - TD3 | Tablue | Guiding Software	Duplicator	1
4	Email Analyzer (Magnet-Axiom)	Email Forensics	1

ANNEXURE-II

TENDER ACCEPTANCE LETTER

(To be given on Company Letter Head)

To,
The Principal

Tender Reference No:_____

Shaheed Sukhdev College of Business Studies
PSP Area-IV, Dr. K. N. Katju Marg, Sector-16, Rohini, Delhi-110089

Sub: Acceptance of Terms & Condition of Tender.

Name of Tender / Work:-
Public Private Partnership on Concession based model as Knowledge partners in Post Graduate Diploma in Cyber Security and Law in SSCBS, PSP Area-IV, Dr. K. N. Katju Marg, Sector-16, Rohini, Delhi-110089 as per description

Dear Sir,

1. I/We have downloaded/obtained the tender document(s) for the above mentioned 'Tender/Work' from the web site(s) namely:
   _____
   _____

   As per your advertisement, given in the above mentioned website(s).

2. I/We hereby certify that I/we have read the entire terms and conditions of the tender documents from Page No.
   ____ to _____ (including all documents like annexure(s), schedule(s), etc.,), which form part of the contract agreement and I/we shall abide hereby by the terms / conditions/ clauses contained therein.

3. The corrigendum(s) issued from time to time by your department / organization would also be taken into consideration, while submitting this acceptance letter.

4. I/we hereby unconditionally accept the tender conditions of above mentioned tender document(s)/corrigendum(s) in its totality/entirely.

5. I/we do hereby declare that our firm has not been blacklisted/debarred by any Govt. Department/Public Sector undertaking.

6. I/we certify that all information furnished by the our Firm is true & correct and in the event that the information is found to be incorrect/untrue or found violated, then your department/organization shall without giving any notice or reason therefore or summarily reject the bid or terminate the contract, without prejudice to any other rights or remedy including the forfeiture of the full said earnest money deposit absolutely.

Yours faithfully,

(Signature of the Bidder, with Official Seal)

ANNEXURE-III: PRE QUALIFICATION DOCUMENTS

The minimum qualifying requirements for the bidders are as under: -

Pre-Qualification Requirement Compliance	(Yes/No/NA)	Detail of proof Attached
Be an entity as Information Technology Risk Assessment and Digital Security Services provider		
Having at least five years of experience in delivery of cyber security services to corporate and Government Department.		
Having experience of handling cyber security projects in Banks, Government Departments / Defence Organisation, Aviation, FMCG and E Commerce in the last three years.		
Be an Empanelled Information Security Auditing Organisation by the Computer Emergency Response Team –India (CERT-In)		
Having a team of cyber security professionals with at least ten full-time OSCP certified professionals		
Having an average annual turnover of INR Two crore or above in the last three financial years		
Have you been blacklisted by any of the Universities/Government Organization(s)/Public Sector Undertaking (s) (PSUs).		
Details of GSTIN and PAN		

Signature & Seal of the Bidder

ANNEXURE-IV : BIDDER INFORMATION

1. Name of the Bidding firm	
2. Full Address & contact details of the firm	
3. Name of the Authorized Signatory for this Bid	
4. Bidder's Proposal number and date	
5. Name and Address of the Person to whom all references Shall be made regarding this tender:	
(a) Telephone	
(b) Fax No.	
(c) E-mail	
(d) Mobile	
Bidder	
Signature of Authorized Signatory	
Name:	

Designation:	
Date:	
Company Seal:	

ANNEXURE-V: COMPLIANCE SHEET FOR Service and Laboratory Tools

1. The installation of all software as required in the course (Annexure A) to operationalize state of the art Cyber Security and forensics lab initially with 50 systems and thereafter as increased by the College of Business studies, University of Delhi, therein.
2. E Toolkit for all the students.
3. Management development programme or faculty development programme (MDP/FDP) organized, if any.
4. Presenter's Manuals for specific classes; Updated reference books and journals to be recommended to students; subscribing national and international journals for referral library; Subject specific toolkits.
5. Professionals for conducting Webinars and International resource person from academia/ industry (preferably on virtual platform)
6. Suggest professionals having Master's degree in Computer Science or Computer Application or B.Tech. Computer Science/Electronics and certified cyber security experts with OSCP certification from an organization of repute and having atleast one year of corporate experience of handling cyber security projects for engagement as guest/ visiting faculty. Payment to expert/guest/visiting faculty shall be paid on per lecture basis as approved by competent authority on monthly basis (INR 4000 per lecture of 60 minute duration) by the college for delivering the content to students of PGDCSL.
7. Research & Development know-how pertaining to cyber security training in University.
8. Industrial visit (except travelling, boarding and lodging), if any.
9. Organizing annual program or event, if any, related to cyber security along with the students of College of Business Studies, University of Delhi and sponsors.
10. Provide placement opportunities each year to students completing the PGDCSL successfully.

LABORATORY Tools I : Web Application Security

Sr. No.	Tool Name	Category	Quantity
1	Metasploit Framework Pro	Penetration Testing	2
2	Burp Suite Pro	Web VA	2
3	Acunetix Web Vulnerability Scanner	Web VAPT	2
4	Netsparker Web Vulnerability Scanner	Web VAPT	2

5	Web Lab Attack Server*	Attacks Practice	2
6	Checkmark Secure Source Code Analyzer	Secure Source Code Reviewer	1

LAB Tools II : Network VAPT Security

Sr. No.	Tool Name	Category	Quantity
1	Nessus Vulnerability Scanner	Network Scanner	2
2	Alpha Cards – External USB Wifi	Wireless Security	2
3	Raspberry Pi 3 Model B	Network Security/IoT	2
4	D-Link DIR-615 Wireless N 300 Router	Network Security	2

LAB Tools III : Cyber Forensics

Sr. No.	Tool Name	Category	Quantity
1	FTK 7.0 Toolkit	Forensic Evidence Collector	1
2	Cellebrite Mobile Forensic Toolkit (UFED) for PC	Mobile Forensic	1
3	DVR Duplicator - TD3 | Tablue | Guiding Software	Duplicator	1
4	Email Analyzer (Magnet-Axiom)	Email Forensics	1

Signature & Seal of the Bidder

ANNEXURE-VI: BILL OF QUANTITY (BOQ)

1. Price bid format is provided as BoQ_XXXX.xls along with this tender document at https://eprocure.gov.in/eprocure/app. Bidders are advised to download this BoQ_XXXX.xls as it is and quote their offer/rates in the permitted column and upload the same in the Price bid. Bidder shall not tamper/modify downloaded price bid template in any manner. In case if the same is found to be tempered/modified in any manner, tender will be completely rejected and Bid Security would be forfeited and tenderer is liable to be banned from doing business with the Purchaser.
2. The Bid shall be quoted in percentage of share in application money received for the program wherein the private partner shall act as knowledge partner.
3. The percentage shall be inclusive of all taxes and duties. Any subsequent revision in the statutory taxes, fees, etc. shall be the responsibility of the Bidder.
4. In case of any discrepancy in the amounts indicated in figure and word the amount in word shall be considered for evaluation.
5. In case of any discrepancy in calculation of total amount, unit price quoted in words will be considered for computation.
6. The quoted percentage shall remain firm throughout the validity period of the bid and no revision is permissible for any reason.

ANNEXURE-VII: LIST OF DEVIATIONS

(Please note that Purchaser will not evaluate any deviation mentioned elsewhere in the bid except as mentioned hereunder)

We certify that the systems/services offered by us for this Bid conforms to the specifications stipulated by you with the following deviations

List of deviations

Sl. No.	Deviation

Signature & Seal of the Bidder

(If left blank it will be construed that there is no deviation from the specifications given above)

ANNEXURE-VIII: DETAILS OF SERVICE SUPPORT IN DELHI/NCR

Sl No.	Location of support office In Delhi / NCR	Service Centre Telephone No. /Fax Number	Type of Support Centre [OEM(O), ASP (A), Franchise (F)]

Signature & Seal of the Bidder

ANNEXURE-IX: DETAILS OF SUPPLY, TURNOVER & PROFIT

Work Experience (During last three year)

Name & Address of The Organization	Order No. & Date	Items & Quantity	Value of the Order	Date of Completion	Attach Copy of the Award of Contract

Signature & Seal of the Bidder

ANNEXURE-X: UNDERTAKING FOR TECHNICAL BID

(On the Letter Head of the Firm submitting the Bid)

BID NO……..

To,
The Principal, Shaheed Sukhdev College of Business Studies
PSP Area-IV, Dr. K. N. Katju Marg, Sector-16, Rohini, Delhi-110089
Dear Madam,

1. I/We have examined and have no reservations to the Bidding Documents, including Corrigenda/Addenda issued.
2. I/We meet the eligibility requirements and have no conflict of interest.
3. I/We have not been suspended nor declared ineligible in India.
4. I/We offer to supply in conformity with the Bidding Documents;
5. I/We offer to supply the items as listed in the Bidding Documents at the price given in the said Price Bid and agree to hold this offer open for a period of 180 days from the deadline for the submission of the Bid.
6. I/we shall be bound by a communication of acceptance issued by you.
7. I/We have understood the Bidding Document and have thoroughly examined the specifications quoted therein and am/are fully aware of the nature of the goods required and my/our offer is to supply the goods strictly in accordance with the specifications and requirements.
8. Receipt Number _____ dated _____ for Rs.200,000/- is enclosed on account of EMD.
   9 Certified that the bidder is:

a) A sole proprietorship firm and the person signing the bid document is the sole proprietor/ constituted attorney of the sole proprietor,

Or

b) A partnership firm, and the person signing bid document is a partner of firm and he has authority to refer to arbitration disputes concerning business of partnership by virtue of the partnership agreement/by virtue of general power of attorney.

Or

c) A company and the person signing the document is the constituted attorney.

(NOTE: Delete whatever is not applicable. All corrections/deletions shall invariable be duly attested by the person authorized to sign the bid document).

10. We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf will engage in any type of fraud and corruption.

Name of the Bidder*** [insert complete name of person signing the Bid]**

Name of the person duly authorized to sign the Bid on behalf of the Bidder***** [insert complete name of person duly authorized to sign the Bid]***

Title of the person signing the Bid **[insert complete title of the person signing the Bid]**

Signature of the person named above **[insert signature of person whose name and capacity are shown above]**

Date signed **[insert date of signing]** day of **[insert month], [insert year]**

*: In the case of the Bid submitted by joint venture specify the name of the Joint Venture as Bidder

**: Person signing the Bid must have the power of attorney given by the Bidder and the same shall be attached.

Yours faithfully,

(Signature & Seal of the bidder)

Dated this day of _____
Address: _____
Telephone No.: _____

Annexure-A

POST GRADUATE DIPLOMA IN CYBER SECURITY AND LAW(PGDCSL)

PREAMBLE

Cyber-security is a niche subject of modern studies wherein this diploma is an advanced Penetration Testing & Information Security Program. The course provides intensive practical sessions to prepare an individual with uncompromising practical knowledge in a simplified and easily graspable manner.

SESSION DURATION

	SEMESTER 1	**SEMESTER 2**
Course	15 weeks	15 weeks
Project	4 weeks	8 weeks
Exams	1	1
Total Academic course duration - 42 weeks excluding examination		

COURSE CONTENT

Semester I	**Semester II**
● Fundamentals of Computer Security ● Networking Basics and Network Security ● Fundamentals of Web Designing and Web Application Security ● Cryptography ● Cloud Fundamentals and Cloud Security ● Project 1	● Mobile Eco System Security ● Internet of Things Security (IoT) ● Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques ● Cyber Laws and Forensics ● Information Security Compliance Management ● Project 2

The schedule of papers prescribed for two semesters shall be as follows:

Semester I

Papers		Hrs. For lectures and labs	Total marks	Marks		
Paper No.	Title			Internal assessment	Practical	Written Exam
1	Fundamentals of Computer Security	60 lectures	100	20	40	40
2	Networking Basics and Network Security	60 lectures	100	20	40	40
3	Fundamentals of Web Designing and Web Application Security	60 lectures	100	20	40	40
4	Cryptography	60 lectures	100	20	40	40
5	Cloud Fundamentals and Cloud Security	60 lectures	100	20	40	40
6	Project 1	4 weeks	100			

Semester II

Papers		Hrs. For lectures and labs	Total marks	Marks		
Paper No.	Title			Internal assessment	Practical	Written Exam
1	Mobile Eco System Security	60 lectures	100	20	40	40
2	Internet of Things Security	60 lectures	100	20	40	40
3	Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques	60 lectures	100	20	40	40
4	Cyber Law & Forensics	60 lectures	100	20	40	40

5	Information Security Compliance Management	60 lectures	100	20	40	40
6	Project 2 + Internship	8 weeks	100			

Note: Each lecture will be of 60 minutes duration.

SCHEME OF EXAMINATIONS

English shall be the medium of instruction and examination.

1. Examinations shall be conducted at the end of each Semester as per the Academic Calendar notified by the University of Delhi
2. The system of evaluation shall be as follows:
   2.1. Each paper will carry 100 marks, of which 20 marks shall be for internal assessment based on a combination of classroom participation, project work, seminar, term papers, tests, and attendance. The weightage given to each of these components in a combination shall be decided and announced at the beginning of the semester in consultation with the faculty of the concerned paper. The system so decided will be communicated by the Institute for Cyber Security and Laws.
   2.2. The remaining 80 marks in each paper shall be awarded on the basis of a practical and written examination of 40 marks each at the end of each semester.

PASS PERCENTAGE & PROMOTION CRITERIA

1. The minimum marks required to pass any paper in a semester shall be 50% in each paper and 50% in aggregate of a semester.
2. **Semester to Semester Promotion:** Students shall be required to fulfil the Part to Partpromotion criteria. Students shall be allowed to be promoted from semester I to semester II, provided s/he has passed at least 60 per cent of the papers in the course of the current semester including project.

DIVISION CRITERIA

Successful candidates will be classified on the basis of the combined results of Semester -I and Semester -II examinations as follows:

- Candidates securing **60% and above**: I Division
- Candidates securing **50% or more but less than 60%**: II Division

ATTENDANCE REQUIREMENT

Attendance in lectures, tutorials, seminars etc. arranged by the Centre for Cyber Security and Laws from time to time, is mandatory according to the Internal Assessment requirement as per University rules. The marks for attendance shall be awarded on the basis of existing norms as per the Internal Assessment Scheme of University of Delhi.

Semester - 1
Paper 101: Fundamentals of Computer Security

Marks: 100 **Lectures 60**

Objective: This course will be responsible to lay the foundation for creating comprehensive understanding in the field of cyber security. With a view that incumbents in this diploma course are from varied disciplines, this paper will set the level field for all the students to be able to come at par and move together as they must go deeper into hard-core cyber security topics during the course duration.

Unit I: Computers and Cyber Security

Introduction to Computers, Computer History, Software, Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Linux/Mac Terminal and Commands, Basic Computer Terminology, Computer Security models, Computer Security Terms, Computer Ethics, Business and Professional Ethics, Need for cyber security; Cyber Frauds and crimes, Digital Payments, Various Search Engines, Introduction to Auditing, Deep Web, VAPT, Smartphone Operating systems, introduction to compliances ,Globalization and border less world.

Unit II: Python Scripting and PHP Basics

Python Basics, Variables and Types, Lists, Basic Operators, String Formatting, Basic String Operations, Conditions, Loops, Functions, Classes and Objects, Dictionaries, Modules and Packages.

Unit III: Cyber Laws

Need for Cyber Regulations; Scope and Significance of Cyber laws : Information Technology Act 2000; Network and Network Security, Access and Unauthorised Access, Data Security, E Contracts and E Forms. Penal Provisions for Phishing, Spam, Virus, Worms, Malware, Hacking, Trespass and Stalking; Human rights in cyberspace, International Co-operation in investigating cybercrimes.

Unit IV: Encoding

Encoding: Charset, ASCII, UNICODE, URL Encoding, Base64, Illustration: ISBN/ QR Code/ Barcode, Binary hamming codes and Binary Reedmuller codes.

Unit V: Web Application Architecture

HTML Basics, XAMPP Server Setup, Hosting Websites Linux, Apache, Virtualisation, Server Configurations, Web Application Firewalls..

Suggested Readings:

1. Langtangen, H.P. (2012). *Python Scripting for Computational Science* (4th Ed.). Springer
2. Behrouz A. Forouzan (2004). *Data communication and Networking*. Tata McGraw-Hill.
3. Kurose, James F. & Ross, Keith W. (2003). *Computer Networking: A Top-Down Approach Featuring the Internet* (3rd Ed.). Pearson Education.
4. Shklar, L. & Rosen, R. (2009). *Web Application Architecture: Principles, Protocols and Practices* (2nd Ed.). John Wiley & Sons.
5. Craig, B. (2012). *Cyber Law: The Law of the Internet and Information Technology.* Pearson.
6. Sharma J. P. & Kanojia S. (2016). *Cyber Laws.* New Delhi: Ane Books Pvt Ltd.
7. Paintal, D. *Law of Information Technology*. New Delhi: Taxmann Publications Pvt. Ltd.
8. Forbes, A. (2015). *The Joy of PHP: A Beginner's Guide to Programming Interactive Web Applications with PHP and mySQL* (4th Ed.). Plum Island Publishing LLC.
9. Shema, M. (2012). *Hacking Web Apps: Detecting and Preventing Web Application Security Problems.*
10. Peterson. W.W, (1972), *Error Correcting Codes,* MIT Press
11. Hill. R, (1980), *A First Course in Coding Theory,* Oxford University Press.
12. Macwilliams F J and Sloane N J A, (2013), *Theory of Error Correcting Codes*, North Holland Elsevier Science Ltd

Semester - 1
Paper 102: Network Basics and Network Security

Marks: 100 **Lectures 60**

Objective: This course aims at teaching students about the fundamentals and distinctions of network building along with setup of present day networks in complex environments. The networks today are vulnerable to various attacks and the course aims at acquainting students with the techniques used by

hackers for network attacks and also the techniques adopted in order to guard the entire infrastructure against varied attacks.

Unit I: Introduction to Network Security

Types of networks, IP Address, NAT , IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP IP Model, Routers , Switches, Endpoint solutions, Access Directory, TOR Network. Networking Devices (Layer1,2,3) - Different types of network layer attacks– Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails) – IDS,IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based).

Unit II: Virtual Private Networks

VPN and its types –Tunneling Protocols – Tunnel and Transport Mode –Authentication Header-Encapsulation Security Payload (ESP)- IPSEC Protocol Suite – IKE PHASE 1, II – Generic Routing Encapsulation(GRE). Implementation of VPNs.

Unit III: Network Attacks Part 1

Network Sniffing, Wireshark, packet analysis, display and capture filters, ettercap, DNS Poisoning, ARP Poisoning, Denial of services, Vulnerability scanning, Nessus, Network Policies, Open VAS, Sparta,Network Scanning Report Generation, System hardening, secure system configurations, SSL Striping, Setup network IDS/IPS, Router attacks, VPN Pentesting, VOIP Pentesting,

Unit IV: Network Attacks Part 2

Network Exploitation OS Detection in network, nmap, open ports, filtered ports, service detection, metasploit framework, interface of metasploit framework, network vulnerability assessment, Evade anti viruses and firewalls, metasploit scripting, exploits, vulnerabilities, payloads, custom payloads, nmap configuration, Social Engineering toolkit, Xero sploit Framework, exploits delivery. End Point Security.

Unit V: Wireless Attacks

Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentication, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP , WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework

Suggested Readings:

1. Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security, Private communication in public world* (2nd Ed.). PHI

2. Monte, M. (2015). *Network Attacks and Exploitation: A Framework*. Wiley.

3. Perez, Andre. (2014). *Network Security*. Wiley.

4. Stallings, W. (2006). Cryptography and Network Security: Principles and Practice (5th Ed.). Prentice Hall

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1
Paper 103: Fundamentals of Web Designing and Web Application Security

Marks: 100 **Lectures 60**

Objective: Moving from networks the most important component any technology stack is the software which is positioned at the top of infrastructure. We will start with the necessities of how software applications are built, where students will understand and build their applications to have the real world feel on how the internet stack is working, along with showing them real loopholes while coding himself so that they understand the real world attacks which are possible on applications, and simulate them so that they can themselves come to conclusions and understand the best practices involved in application security.

Unit I: Web Designing and Penetration Testing Process

Scope Understanding, Liabilities and Responsibilities, Allowed Techniques, Deliverables, OWASP Top 10 Attack Testing Guidelines, Reporting- Executive Summary, Risk Exposure over time, Successfully Attacks by whom, Vulnerability causes, Vulnerability report, Remediation report, Report Design Guidelines, Malware Analysis.

PHP Basics: Variables, data types, strings, constants, operators, if else, else if statements, switch, while loops, for loops, functions, arrays, php forms, form handling, validation, form input page with database attachment, XAMPP Server Setup.

Unit II: Web Application and Information Gathering

HTTP Request, Response, Header Fields and HTTPS, Understanding Same Origin, Cookies, Sessions, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration, fingerprinting frameworks, hidden resource enumeration, security misconfigurations, google hacking database, Shodan HQ.

Unit III: Web Application Attacks Part I: SQL Injections & Cross Site Scripting

SQL Statements, Finding SQL Injections, Exploiting SQL Injections, Bypass Authentication, Xpath Injection, Error Based Injection, Double Query Injection, Time Based injections, Union Based Injections, SQL Map, Mitigation plans, SQLi to Server Rooting, Advance MY-SQL and MS-SQL Exploitation. Cross Site Scripting: Anatomy of an XSS Exploitation, Reflected XSS, Persistent XSS, DOM based XSS, Browsers and XSS, Cookie Stealing, Defacements, Advanced Phishing attacks, BeEF Framework, Mitigation.

Unit IV: Web Application Attacks Part II

Single factor and two factor authentication, dictionary and brute force attacks, storing hashes, blocking malicious request, user enumeration, random password guessing, remember me functionality, no limit attempts, password reset feature, logout flaws, CAPTCHA, insecure direct object reference and security, missing function level access control, unvalidated redirects and forwards, Session ID, LFI and RFI ,Session Attacks via packet sniffing or accessing via web server and Fixation, CSRF (Cross Site Request Forgery), Pentesting Flash -based applications, HTML 5, Cross Origin Resource Sharing Policy, Cross Windows Messaging, Web Storage, Web Sockets, Sandbox, Path Traversal, Arbitrary file uploading, Clickjacking, HTTP Response Splitting, Business Logic Flaws, denial of services attacks.

Practical: This paper will have 30 lectures for the practical work.

Suggested Readings:

1. Shema, M. & Adam. (2010). *Seven deadliest web application attacks*. Amsterdam: Syngress Media.
2. Stuttard, D. & Pinto, M. (2011). *The web application hacker's handbook: Discovering and exploiting security flaws* (2nd ed). Indianapolis, IN: Wiley, John & Sons.
3. Heiderich, M., Nava E.A.V., Heyes, G., & Lindsay, D. (2011). *Web application obfuscation*. Amsterdam: Syngress Media,U.S.
4. Sullivan, Bryan (2012). *Web Application Security, A Beginner's Guide*. McGraw- Hill Education.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1
Paper 104: Cryptography

Marks: 100 **Lectures 60**

Objective: After infrastructure and software, the communication in between multiple devices using applications and securing them become most important, cryptography is the mechanism using which we hide the information in public eye site from anybody and is something which is used very popularly almost anything across the internet. So we start with fundamentals of what is cryptography and how cryptography algorithms work and then come to real world scenarios on how currently our data processed on the internet is secured from the eyes of an intruder. Further, the paper enables the students to use cryptography in the most extensive and elaborate manner.

Unit I: - Classical Ciphers

Ceaser Cipher, Vegnere Cipher, Rail-fence Cipher, Row Transposition Cipher.
Requirement and Basic Properties, Main Challenges, Confidentiality, Integrity, Availability, Non-Repudiation,

Unit II: Secret Key Cryptography

Data Encryption Standard-Symmetric Ciphers (Stream Cipher &Block cipher) Advanced Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family.

Unit III: Public Key Cryptography and Bitcoins

Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic-Elliptic curve cryptography, cryptanalysis.
Bitcoin introduction, working, blockchain crucial to bitcoin, block chain operation with bitcoins, bitcoin glossary, bitcoin wallets, setup for bitcoin payments, bitcoin mining.

Unit IV: Message authentication code and Hash Functions

Message authentication code Authentication functions, Hash functions-Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard). Digital Certificate and Public Key Infrastructure.

Suggested Readings:

1. Delfs, H. & Knebl, H. (2001). *Introduction to Cryptography: Principles and Applications*. Springer-Verlag Berlin and Heidelberg GmbH & Co.

2. Stallings, W. (2010). *Cryptography and network security: Principles and practice* (5th ed.) Boston: Prentice Hall.

3. Menezes, A.J., Oorschot, P. Van & Vanstone, S.A. (1997). *The Handbook of Applied Cryptography*. CRC Press.

4. Schneier, B. (1995). *Applied cryptography, Protocols, algorithms and source code in C* (2nd ed.). New York: John Wiley & Sons.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1
Paper 105: Cloud Fundamentals and Cloud Security

Marks: 100 **Lectures 60**

Objective: The purpose of the course is to make students understand and comprehend the revolutionizing concept of CLOUD in the cyber world with a view to enable them with achieving cloud security. It also aims at developing expertise amongst students with the cloud architecture as well as the security concerns for organizations planning a move towards Cloud or planning to enhance their cloud security.

Unit I: Introduction to Cloud Computing
Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vsprivateclouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications.

Unit II: Cloud Application Architecture
Technologies and the processes required when deploying web services; Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages.

Unit III: Cloud Services Management
Reliability, availability and security of services deployed from the cloud.
Performance and scalability of services, tools and technologies used to manage cloud services deployment; Cloud Economics: Cloud Computing infrastructures available for implementing cloud based services. Economics of choosing a Cloud platform for an organization, based on application requirements, economic constraints and business needs. Discuss industry cases including open sources.

Unit IV: Cloud Application Development
Service creation environments to develop cloud based applications. Development environments for service development; Amazon, Azure, Google App.Applicability of laws to data stored outside the nation's boundary.

Unit V: Cloud IT Model

Analysis of Cases while deciding to adopt secure cloud computing architecture. Appropriate cloud requirements. Secure Cloud based service, Applications and development platform deployment so as to improve the total cost of ownership (TCO)

Suggested Readings:

1. Rittinghouse, J.W. & Ransome, J.F. (2010). *Cloud Computing: Implementation, Management, and Security*. CRC Press.

2. Rountree, D. & Castrillo, I. (2013). *The Basics Of Cloud Computing: Understanding The Fundamentals Of Cloud Computing In Theory And Practice*. Syngress, Elsevier

3. Stallings (2016). *Cryptography & Network Security*. Paperback.

4. Vacca, J. (2016). *Cloud Computing Security: Foundations and Challenges*. CRC Press

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1
Paper 106: Project - 1

Marks: 100 Duration: 4 Weeks

Rules for the Project:

- The students would develop their project individually and get the topic approved by the head/ director of the centre. For the purpose of approval, they have to submit their project titles and proposals with the name of internal or external guides to the head/ director of the centre within forty five days of the commencement of the semester. In case, if the student proposal is rejected, the revised proposal, is required to submit and get it sanctioned within next seven days. Failing to do this, He/she will not be qualified for this subject.

- The students have to report to the guide for at least three times during the project lifespan with the progress report duly signed by the internal guide. Moreover they have to submit the progress reports with the final project report at the time of external examination.

- The external examiners appointed by the head/ director of the Institute shall award the marks out of 20 on the basis of the Presentation, Demonstration, Viva-Voce, and out of 40 on the basis of Project Report. The internal guide shall award out of 40 Marks.

Semester 2
Paper 201: Mobile Eco- System Security

Marks: 100 **Lectures 60**

Objective: At time when companies are looking at not only a mobile first approach but a mobile only approach, the cell phone revolution has hit both the enterprise and the consumer market in a massive way. Its entire eco system needs to be very carefully understood , and the various attacks which can be possible at each stage needs to be carefully, practically performed in order to understanding how to protect the entire mobility ecosystem, which is going to be one of the most important pillars of transforming an organisation into a digital organisation.

Unit I: Introduction to Mobile Eco-System Security
Mobile Security Model, Enterprise Mobile Environment, Mobile Crypto Algorithm.

Unit II: Mobile Eco-System Technology
Mobile Devices - features and security concerns, Platforms, Applications - development, testing and delivery

Unit III: Mobile Eco-System Networks
Cellular Network - baseband processor and SIM card, GSM encryption and authentication and other attacks, WIFI Networks - public hotspots and enterprise WLANs, SSL/TLS , Web Technologies - server-side and client side web applications

Unit IV: Management
Enterprise Mobility Program, Transactions Security, File Synchronization and Sharing, Vulnerability Assessments, BYOD Device Backup, Data Disposal/Sanitization, NAC for BYOD, Container Technologies, Exchange ActiveSync (EAS), Mobile Authentication, Mobile Management Tools

Unit V: Scenario Testing
Cellular Attacks, Attacking Web Interface, Wireless Attacks, SSL attacks, Android, iOS

Suggested Readings:

1. Fried, S. (2010). *Mobile device security: A comprehensive guide to securing your information in a moving world*. Boca Raton, FL: Auerbach Publications.
2. Stuttard, D. & Pinto, M. (2011). *The web application hacker's handbook: Discovering and exploiting security flaws* (2nd ed.). Indianapolis, IN: Wiley, John & Sons.
3. Dwivedi, H., Clark, C., & Thiel, D. (2010). *Mobile application security*. New York: McGraw-Hill Companies.

Semester 2
Paper 202: Internet of Things Security (IoT)

Marks: 100 **Lectures 60**

Objective: The human race is going to go through a major transformation in the next ten years thanks to the internet of thing , when such a transformation happens, where internet and technology are going to touch possibly every aspect of our life , the security of the same would be of highest importance , here we will dwell with most popular IoT devices available in the market at present and their security concerns along with potential hacks that can be performed on such devices and to ensure its security according to best global practices.

Unit I: Introduction

Requirement and Basic Properties in Internet of Things, Primary challenges in security maintenance, Confidentiality, Integrity, Availability, Non-Repudiation.

Unit II: Architecture of Internet of Things

Device - device, Device - Cloud, Device - Gateway, Gateway - Cloud, Cloud – Backend - Applications

Unit III: Security Classification and Access Control

Data classification (Public and Private), Internet of Things Authentication and Authorization, Internet of Things Data Integrity

Unit IV: Attacks and Implementation of Internet of Things

Denial of Service, Sniffing, Phishing, DNS Hijacking, Pharming, Defacement, Firmware of the device, Web Application Dashboard , Mobile Application Used to Control, Configure and Monitor the Devices

Unit V: Security Protocols and Management

Firmware of the device, Web Application Dashboard , Mobile Application Used to Control, Configure and Monitor the Devices, Identity and Access Management, Key Management

Suggested Readings:

1. Russell, B. (2016). *Practical Internet of Things Security***.** Packt Publishing Limited
2. FeiHu (2016). *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations***.** CRC Press
3. Hersent, O., Boswarthick, D., & Elloumi, O. (2015). The Internet of Things: Key Applications and Protocols. Wiley
4. Pfister, C. (2011). *Getting Started with the Internet of Things*. Shroff Publisher.

Semester 2

Paper 203: Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques

Marks: 100 **Lectures 60**

Objective: What Internet of things would be to consumers, SCADA and Industrial control systems would be to enterprises, the heavy machinery that we have been thinking of its intelligent management is going to be completely taken over by the technology. Although it looks like a great boon however if take over, we have seen in the past some of the national critical infrastructures of some very developed countries being compromised and the damages happening which are irreversible hence it becomes most important to understand the cyber risks that such technologies posses and to give the education of the best practices followed for securing such technologies.

Unit I: Introduction

Network Segmentation and Segregation , Boundary Protection, Firewalls , Logically Separated Control Network , Network Segregation, Recommended Defence-in-Depth Architecture, General Firewall Policies for ICS , Recommended Firewall Rules for Specific Services , Network Address Translation (NAT), Specific ICS Firewall Issues , Unidirectional Gateways , Single Points of Failure , Redundancy and Fault Tolerance , Preventing Man-in-the-Middle Attacks , Authentication and Authorization , Monitoring, Logging, and Auditing, Monitoring, Logging, and Auditing , Response, and System Recovery

Unit II: Network Segregation

Dual-Homed Computer/Dual Network Interface Cards (NIC) , Firewall between Corporate Network and Control Network , Firewall and Router between Corporate Network and Control Network , Firewall with DMZ between Corporate Network and Control Network , Paired Firewalls between Corporate Network and Control Network , Network Segregation Summary

Unit III: Recommended Firewall Rules for Specific Services

Domain Name System (DNS) , Hypertext Transfer Protocol (HTTP) ,FTP and Trivial File Transfer Protocol (TFTP) ,Telnet ,Dynamic Host Configuration Protocol (DHCP) , Secure Shell (SSH) ,Simple Object Access Protocol (SOAP) , Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP) ,Distributed Component Object Model (DCOM),SCADA and Industrial Protocols: DNP3 Protocol. Smart Grid Security.

Unit IV Information Hiding Techniques

Introduction to Steganography, Watermarking. Differences between Watermarking and Steganography, A Brief History. Digital Steganography, Applications of Steganography, Covert Communication, Techniques of steganography(for Text and Image) . Steganographic Software: S-Tools, StegoDos, EzStego, Jsteg-Jpeg.

Unit V : Digital Water Marking

Classification in Digital Watermarking, Classification Based on Characteristics: Blind versus Nonblind, Perceptible versus Imperceptible, Private versus Public, Robust versus Fragile, Spatial Domain-Based versus Frequency Domain-Based. Classification Based on Applications: Copyright Protection Watermarks, Data Authentication Watermarks, Fingerprint Watermarks, Copy Control Watermarks, Device Control Watermarks. Watermarking Techniques for Visible and Invisible Watermarks. Watermarking tools: uMark, TSR Watermark. Steganalysis

Suggested Readings

1. Macaulay, T. & Singer, B. (2016). *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. Boca Raton, FL: CRC Press.

2. Langner, R. (2011). *Robust control system networks: How to achieve reliable control after Stuxnet*. New York: Momentum Press.

3. Knapp, E.D. & Langill, J.T. (2011). Industrial network security: Securing critical infrastructure networks for smart grid, SCADA , and other industrial control systems. Waltham, MA: Syngress Media, U.S.

4. Katzenbeisser, S. & Fabien A P. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Petitcolas, Artech House.

5. *Cox, I., Miller, M., Bloom, J., Fridrich, J. & Kalker, T. (2007). Digital Watermarking and Steganography* (2nd Ed.). Elsevier.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester 2
Paper 204: Cyber Law and Forensic Evidence

Marks: 100 **Lectures 60**

Objective: The paper aims to create the basic clarity and understanding of cybercrimes and cyber security laws to the professionals learning the ethical hacking programme. The paper would address and emphasise on the activities leading to infringement of individual or organisational privacy. Further, the paper intends to create highly sensitised professionals who can be responsible for handling the cyber security issues pertaining to varied domains and dealing in forensics diligently.

Unit I: Introduction to Cyberspace, Cybercrime and Cyber Law

The World Wide Web, Web Centric Business, E Business Architecture, Models of E Business, E Commerce, Threats to virtual world. Cyber Crimes& social media, Cyber Squatting, Cyber Espionage, Cyber Warfare, Cyber Terrorism, Cyber Defamation. Online Safety for women and children, Misuse of individual information. Objectives, Applicability, Non applicability and Definitions of the Information Technology Act, 2000.

Unit II: Regulatory Framework of Information and Technology Act 2000

Digital Signature, E Signature, Electronic Records, Electronic Evidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal.(Rules announced under the Act)

Unit III: **Offences and Penalties**

Offences under the Information and Technology Act 2000, Penalty and adjudication. Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed).Limitations of Cyber Law.

Unit IV: Fundamentals of Cyber Forensics

Cyber Forensic Basics- Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology Data and Evidence Recovery- Introduction to Deleted File Recovery, Formatted Partition Recovery

Unit V: Data Recovery Tools, Data Recovery Procedures and Ethics

Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility, Document a Chain of Custody and its importance, Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Data Protection and Privacy, Recover Swap Files/Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Toolkit etc, Use computer forensics software tools to cross validate findings in computer evidence-related cases.

Unit VI: Cyber Forensics Investigation

Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking, Cracking with GPU Systems , Hashcat. Work on open Source, Commercial tools and Cyber range.

Suggested readings

1. Craig, B. *Cyber Law: The Law of the Internet and Information Technology.* Pearson Education
2. Paintal, D. *Law of Information Technology*. New Delhi: Taxmann Publications Pvt. Ltd.
3. Lindsay, D. (2007). *International domain name law: ICANN and the UDRP*. Oxford: Hart Publishing.

4. Sharma J. P, & Kanojia S. (2016). *Cyber Laws.* New Delhi: Ane Books Pvt. Ltd.

5. Duggal, P. *Cyber Laws*. (2016) Universal Law Publishing.

6. Kamath, N. (2004). *Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (2nd ed.)*. Delhi: Universal Law Publishing Co.

7. Stephenson, P.R. & Gilbert, K. *Investigating computer- related crime a handbook for corporate investigators*. Boca Raton, FL: Taylor & Francis.

8. Prosise, C. & Mandia, K. (2003). Incident response & computer forensics (2nd ed.). New York, NY: McGraw-Hill Companies.

Latest Editions of the Suggested Readings along with discussion material by the Faculty.

Semester 2
Paper 205: Information Security Compliance Management

Marks: 100 **Lectures 60**

Objective: In view of providingtechnical superiority essentially be complimented with the appropriate compliance advancement to maintain hygiene from the point of view of cyber security.Complianceshaveincreasinglycoming up not in just financial or aviation space but also in conventional industries like manufacturing, real estate among others and hence its of tremendous importance for a cyber-security professional to have comprehensive knowledge of the most important compliances and the modus operandi from people, process and technology to get through a compliance check.

Unit I: Introduction to Information Security Management System (ISMS) - ISO/IEC 27001
Critical Appraisal of ISO 9000, Normative, regulatory and legal framework related to information security Fundamental principles of information security,ISO/IEC 27001 certification process,Information Security Management System (ISMS), detailed presentation of the clauses 4 to 8 of ISO/IEC 27001

Unit II: Planning and Initiating an ISO/IEC 27001 audit
Fundamental audit concepts and principles, Audit approach based on evidence and on risk, Preparation of an ISO/IEC 27001 certification audit, ISMS documentation audit, Conducting an opening meeting

Unit III: Conducting an ISO/IEC 27001 audit
Communication during the audit, Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration and evaluation, Audit test plans, Formulation of audit findings, Documenting nonconformities

Unit IV: Concluding and ensuring the follow-up of an ISO/IEC 27001 audit
Audit documentation, Quality review, Conducting a closing meeting and conclusion of an ISO/IEC 27001 audit, Evaluation of corrective action plans, ISO/IEC 27001 Surveillance audit, internal audit management program

Unit V: PCI DSS, HIPPA
Security Management Process, Risk Analysis Risk Management, Information System Activity Review, Assigned Security Responsibility, Authorization and/or Supervision, Termination Procedures, Access Authorization, Access Establishment and Modification, Protection from Malicious Software, Log-in Monitoring, Password Management, Response and Reporting, Contingency Plan Evaluation, Facility Access Control and Validation Procedures, Unique User Identification, Emergency Access Procedure, Automatic Logoff Encryption and Decryption, Audit Controls, Data Integrity, Person or Entity Authentication, Integrity Controls Encryption

Unit VI Intellectual Property Rights
Intellectual Property Rights: Types and Issues related to IPR, Policy framework in India and Abroad, Bitcoin and law enforcement.

Suggested Readings:

1. Godbole, N. *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*. Wiley
2. Calder, A. (2009*). Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide* (2nd Ed.). Van Haren Publishing
3. Humphreys, E. (2007). *Implementing the ISO / IEC 27001 Information Security Management System Standard*. Artech House Publishers.
4. Watkins, S. G. (2013). *An Introduction to Information Security and ISO 27001: A Pocket Guide*. IT Governance Publishing.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Paper 206: Project - 2

Marks: 100 **Duration: 8 Weeks**

Rules for the Project:

- The students would develop their project individually and get the topic approved by the head/ director of the centre. For the purpose of approval, they have to submit their project titles and

proposals with the name of internal or external guides to the head/ director of the centre within twenty one days of the commencement of the semester. In case, if the student proposal is rejected, the revised proposal is required to submit and get it sanctioned within next seven days. Failing to do this, He/she will not be qualified for this subject.

- The students have to report to the guide for at least five times during the project lifespan with the progress report duly signed by the internal guide. Moreover they have to submit the progress reports with the final project report at the time of external examination.

- The external examiners appointed by the head/ director of the Institute shall award the marks out of 20 on the basis of the Presentation, Demonstration, Viva-Voce, and out of 40 on the basis of Project Report. The internal guide shall award out of 40 Marks.