

Tender NO: 11BRD/4724/1/IT BM-II DATED 06 Dec 24

GOVERNMENT OF INDIA
INDIAN AIR FORCE

DEPOT INFORMATION TECHNOLOGY
11BRD AIRFORCE STATION OJHAR

INVITATION OF BIDS FOR PROCUREMENT OF
IT TRAINING COURSES UNDER TWO BID SYSTEM

REQUEST FOR PROPOSAL (RFP): 11BRD/4724/1/IT BM-II DATED 06 Dec 24

1. The Bids are invited on behalf of the President of India through '**Open Tender Enquiry Under Two Bid System**' by the Depot Information Technology 11 BRD, AF for IT training courses as listed in Part -II of this RFP. The tender reference number 11BRD/4724/1/IT BM-II dated 06 Dec 24 can be downloaded at <https://eprocure.gov.in/eprocure/app> Please super scribe the above mentioned Title, RFP number and date of opening of the Bids on the sealed envelope to avoid the Bid being declared invalid.

2. The address and contact numbers for sending bids, Mandatory Documents & seeking clarification as explicitly asked for in this RFP are given below:-

- (a) Bids/queries to be addressed to the following:-

Air Officer Commanding,
11 BRD
Air Force Station
Ojhar, Nashik- 422221

- (b) Name & designation of the contact person:

Depot Information Technology Officer (DITO),
11 BRD,
Air Force Station, Ojhar

- (d) Telephone no. of the contact person: **02550 276641 Extn: (11BRD) 7450/7455**

- (e) E-mail IDs of the contact person: **tapti.166@gov.in**

3. This RFP is divided into five parts as follows:-

- (a) Part I - Contains general information and instructions for the bidders about the RFP such as time, place of submission and opening of tenders, validity period of tenders etc.
(b) Part II - Contains essential details of the items/services required, such as the schedule of requirements (SOR), technical specifications, delivery period, mode of delivery and consignee details.
(c) Part III - Contains standard conditions of RFP, which will form part of the contract with the successful bidder.


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

(d) Part IV- Contains special conditions applicable to this RFP and which will also form part of the contract with the successful bidder.

(e) Part V- Contains evaluation criteria and format for price bids.

4. Clarification, if any, must be sought in writing from Depot Information Technology, 11BRD, within 07 days of the issue of the RFP. Online queries would be accepted from prospective bidders and can be forwarded online on or before **13 DEC 24 by 1300 Hrs**. The rep of Depot IT would answer all queries which have been raised in writing to Depot Information Technology.

5. This RFP is being issued with no financial commitments and the buyer reserves the rights to change or vary any part thereof at any stage. Buyer also reserves the rights to withdraw the RFP, should it become necessary at any stage.

Please super scribe the above mentioned Title, RFP number and date of opening of the Bids on the sealed envelope to avoid the Bid being declared invalid.



(Jagmohan Kumar)
Wing Commander
Depot IT Officer
For Air Officer Commanding



(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

PART I

GENERAL INFORMATION

1. The critical dates with respect to tender reference no. **11BRD/4724/1/IT BM-II** dated **06 Dec 24** is appended below:-

CRITICAL DATE SHEET			
Sl No	Item	Date	Time
(a)	Publishing of Tender	06 Dec 24	1430 Hrs
(b)	Bid Document Download	06 Dec 24	1430 Hrs
(c)	Clarification Start	06 Dec 24	1000 Hrs
(d)	Clarification End	13 Dec 24	1000 Hrs
(e)	Bid Submission Start	06 Dec 24	1430 Hrs
(f)	Bid Submission End	27 Dec 24	1000 Hrs
(g)	Opening of Technical Bid	27 Dec 24	1100 Hrs
(h)	Opening of Commercial Bid	Will be intimated after acceptance of the Technical Bids	

Note: The sealed Bids should be deposited/reached by the due date and time. Bids received after due date will not be considered. The responsibility to ensure this lies with the Bidders.

2. **Manner of submission of Bids in two bid system:** Sealed Bids should be either dropped in the Tender Box kept near **Main Guard Room, Air Force Station, Ojhar, Nashik-422221** marked as **"Bid for IT Training courses at 11 BRD"** prior to bid submission closing date and time or sent by registered post at the address given above, so as to reach by due date and time. Late tenders will not be considered. No responsibility will be taken for postal delay or non-delivery/non-receipt of Bid documents. Bids sent by FAX or e-mail will not be considered.

3. **Manner of depositing the Bids:** The proposals shall be submitted in single copy. Technical Bid and Commercial Bid Performa are placed at **Annexure 'I' & 'III'** respectively. It is to be noted that Technical and Commercial Bid are to be submitted as per enclosed Performa only, failing which, will lead to rejection of Technical and Commercial Offer. Both the Bids should be sealed in two separate envelopes and suitably **marked as 'Technical Bid / 'Commercial Bid'** giving reference and date of this bid. Bids in which technical and commercial aspects are combined shall not be considered. These two envelopes further are to be enclosed in a combined bigger envelope. This envelope should be marked boldly as:

**"TECHNICAL AND COMMERCIAL BID FOR TENDER NO.
11BRD/4724/1/IT BM-II DATED 06 Dec 24
PROCUREMENT OF IT TRAINING COURSES
DUE ON 27 DEC 2024"**

"NOT TO BE OPENED AT CENTRAL REGISTRY"


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

4. Mandatory Document: The following mandatory documents are to be submitted along with Technical Bid. Non submission of mandatory document would leads to rejection of bids.

- (a) Earnest Money Deposit (EMD)
- (b) GST Reg. Certificate
- (c) Copy of RFP duly stamped and ink signed on all pages
- (d) Tender Acceptance Letter (Annexure-TV of RFP)
- (e) **Certificates/Documents:** All mandatory certificates/documents must be submitted after signature/authentication as per Annexure 'II'. Ink signed annexure 'I' & 'II' is also to be submitted.

5. Institute Profile: The Institute is required to meet the following eligibility criteria to participate and submit the required/relevant certificates to this effects along with the Technical bid: -

- (a) The Institute should not have been blacklisted by any of the offices of Central or State Govt. or any of its customers. (Self-attested certificate to be attached.)
- (b) No legal action should have been taken against the Institute for any cause in any legal jurisdiction in the last five years. (Self-attested certificate to be attached).
- (c) The Institute should have a minimum annual turnover of 10 crore. (Audited annual accounts report of last three financial years)
- (d) Institute should be an authorized training partner with EC Council. (Relevant certificates to be submitted).
- (e) Trainer educational qualifications with minimum 5 years' experience in training of respective subject course. (Relevant certificates to be submitted).
- (f) The institute should be MeitY/ AICTE/ ISO 9001:2015 Certified (Relevant certificates to be submitted)
- (g) Proof of Past Five Training History for same courses (relevant certificates or supply Order to be submitted).
- (h) Institute must have at least 10 years of experience in same field. (Relevant certificates to be submitted)
- (j) Institute must provide a valid verifiable course completion certificate



(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

5. **Time and date for opening of Bids:** At 1200 Hrs. on 27 DEC 24, at Office of Depot IT Officer, Air Force Station, Ojhar, Nashik-422221. (If due to any exigency, the due date for opening of the Bids is declared a closed holiday, the Bids will be opened on the next working day at the same time or on any other day/time, as intimated by the Buyer).

6. **Location of the Tender Box:**

Main Guard Room,
Air Force Station,
Ojhar, Nashik-422221.

7. **Place of opening of the Bids:** Bids will be open at the Office of Depot IT Officer, Air Force Station, Ojhar, Nashik-422221. The Bidders may depute their representatives, duly authorized in writing, to attend the opening of Bids on the due date and time. Rates and important commercial/technical clauses quoted by all Bidders will be read out in the presence of the representatives of all the Bidders. This event will not be postponed due to non-presence of your representative.

8. **Opening of Two Bid System:** It is a two bid system and only the Technical Bid would be opened on the time and date mentioned above. Date of opening of the Commercial Bid will be intimated after acceptance of the Technical Bids. Commercial Bids of only those firms will be opened, whose Technical Bids are found compliant / suitable after Technical evaluation is done by the Technical Evaluation Committee (TEC). The bid opening date will align with the critical date sheet of the RFP available on the Central public Procurement Portal (<https://eprocure.gov.in/eprocure/app>) and Refers to Part I Para 1 of the RFP.

9. **Clarification Regarding Contents of RFP:** - A prospective bidder who requires clarification regarding the contents of the bidding documents shall notify to the Buyer in writing about the clarifications sought not later than 07 days prior to the date of publishing of the Bids. Copies of the query and clarification by the purchaser will be uploaded as corrigendum if required for all prospective bidders.

10. **Forwarding of Bids:** Bids should be forwarded by Bidders under the original memo / letter pad inter-alia furnishing details like TIN number, GST No. and HSN Code, Bank Address with EFT Account, etc. and complete postal & e-mail address of their office. The original RFP format duly stamped and signed by the vendor / firm on all the pages is also to be submitted along with bidders letter pad. (Same can be submitted in the envelope containing Technical Bid only)

11. **Modification and Withdrawal of Bids:** A bidder may modify or withdraw his bid after submission provided that the written notice of modification or withdrawal is received by the Buyer 01 day prior to bid opening date. A withdrawal notice may be sent by fax but it should be followed by assigned confirmation copy to be sent by post and such signed confirmation should reach the purchaser not later than the deadline for submission of bids. No bid shall be modified after the deadline for submission of bids. No bid to be withdrawn in the interval between the deadline for submission of bids and expiration of bid validity period as specified. Withdrawal of the bid during this period will result in forfeiture of Bidder's EMD.



(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

12. **Clarification regarding contents of the Bids:** During evaluation and comparison of bids, the Buyer may, at its own discretion, ask the bidder for clarification of the bid. The request for clarification will be given in writing and no change in prices or substance of the bid will be sought, offered or permitted. No post-bid clarification on the initiative of the bidder will be entertained.

13. **Reasons for Rejection / invalidation of Bids:** The bids would be rejected/invalidated due of the following reasons: -

(a) Non-submission of Commercial/Financial Bid as per prescribed format (as per Annexure 'III')

(b) Canvassing by the Bidder in any form, unsolicited letter and post-tender correction may invoke summary rejection with forfeiture of EMD.

(c) Conditional Bids will not be accepted.

(d) Bids in which technical and commercial aspects are combined shall not be considered.

14. **Unwillingness to quote:** Bidders unwilling to quote should ensure that intimation to this effect reaches before the due date and time of opening of the Bid, failing which the defaulting Bidder may be delisted for the given range of items as mentioned in this RFP.

15. **Validity of Bids:** The Bids should remain valid for **One Hundred Twenty (120) Days** from the last date of submission of the Bids.

16. **Earnest Money Deposit (EMD):** The Bidders are required to submit Earnest Money Deposit (EMD) for an amount of Rs. 2,20,000/- along with bids. The EMD may be submitted in favour of "AIR FORCE PUBLIC FUND A/C OJHAR" in the form of an Account Payee Demand Draft, Fixed Deposit Receipt, Banker's Cheque or Bank Guarantee from any of the public sector banks or a private sector bank authorized to conduct government business as 171 per Form DPM-16 (Available in MoD website and can be provided on request). EMD is to remain valid for a period of forty-five days beyond the final bid validity period. EMD of the unsuccessful bidders will be returned at the earliest after expiry of the final bid validity and latest on or before the 30th day after the award of the contract. The Bid Security of the successful bidder would be returned without any interest whatsoever, after the receipt of Performance Bank Guarantee (PBG) as called for in the contract. EMD is not required to be submitted by those Bidders who are registered with the Central Purchase Organization (e.g. DGS&D), National Small Industries Corporation (NSIC) or any Department of MoD or MoD itself. The EMD will be forfeited if the bidder withdraws or amends, impairs or derogates from the tender in any respect within the validity period of the Bid.

17. **Payment Terms:** Rate quoted by the Firm should include all legitimate taxes. No conditional clauses/ discounts will be considered while deciding the lowest bid. Quotations with conditional clauses will be rejected. No advance payment(s) will be made. The Payment shall be made batch wise i.e. 1st installment of the payment will be released immediately after completion of the 1st batch of course & submission of requisite bills and so on for the next batches.

18. **Deduction of TDS:** TDS shall be deducted from the amount quoted at the prevailing rate while making payment.


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

PART II

ESSENTIAL DETAILS OF ITEMS/SERVICES REQUIRED

1. **Schedule of Requirement.** List of Items (courses) required is appended below (Bidders to ensure that item offered are correctly understood and where required requisite clarification obtained and forwarded along with the offer before tendering their offer): -

(a) Course Schedule:

(i) The RFP is looking for conduct of courses as per the details given out in **Appendix 'A'**. The bidder would ensure that the course content outlined in Appendix 'A' is adhered to. However, the bidders are at liberty to increase the course content based on the latest technology available within the same duration. The detailed course content hour wise is to be submitted by the bidders for each courses.

(ii) The Depot IT, 11BRD can amend schedule, duration, course content and inclusion or deletion of the course. The bidder should be flexible in finalizing the course scheduling with a notice period of minimum one week.

(b) Venue:

(i) The location for conduct of courses given in Appendix 'A' would be at **11 BRD, Air Force Station Ojhar, Nashik**. For this purpose, the bidder has to ensure that they depute one resource for setting up of the classroom at IAF premises.

(ii) Training infrastructure and computers would be provided by Depot IT, 11 BRD. **Required Software, Network environment and Internet connection for training to be provided by bidders.**

(iii) The bidder will be responsible for all expenses incurred by trainers/instructors in relation to the course/program delivery. This includes travel costs, accommodation, meals, local travel between trainer lodging and the training venue.

(c) Instructor: -

(i) The firms should provide efficient instructors and Training Software for each courses.

(ii) If training monitoring team of IAF finds an instructor to be less competent even after commencement/duration of course, he/She is to be replaced immediately (within one day) without affecting the flow of the course.

(iii) Courses are not to be conducted in parallel.

(iv) Qualification of the instructor will be as per attached **Appendix 'B'**. The medium of instruction will be English.

(v) Experience and educational qualifications of the instructor will be certified by the head of the training division of the Bidders.

(d) **Timing:** The details of the courses are as per attached **Appendix 'A'**. In case, during any week, if there is a closed holiday, the bidder should be willing to compensate for these lost days by working on Saturdays. In case the lost days are more, proportional Saturdays should be catered in the course duration. In case of for any unforeseen reasons, if the course schedule is affected for more than 4 days, the bidder should extend the course duration by one week subsequently.

(e) **Batch size:** -The minimum and maximum strength of participant for each batch is 20 (Twenty).

(f) **Courseware:**

(i) The sample Courseware will be provided by institute for perusal of IAF well in advance before commencing courses. Preferably, courseware is to be designed by institute as per the syllabi for a course. The courseware will consist of following:-

(aa) Suitable handouts with ideal details of steps, tips, best practices and precautions in soft and hard copies. The soft copies will be in the adobe acrobat format providing for easy navigation between chapters.

(ab) Lab exercises with ideal answers both soft and hard copies.

(ac) Suggested textbooks.

(ad) Slide shows both soft and hard copies, which do not violate copyright of other organizations.

(ae) Audio/video shows (optional)

(af) Assignments to trainees with ideal answers both soft and hard copies.

(ii) Courseware for the minimum number of participants will be handed over to IAF one week in advance and courseware for remaining participants will be supplied on the first day of the course.

(iii) The installation of network, Internet and configuration of software will be completed one day prior to the commencement of the course.

(iv) The Bidder will provide one set of courseware approved by procurement committee which includes Executive quality Leather writing pads, Training Material (handouts/Pdf), Executive quality genuine Leather office bags(Laptop Bag) size 15-16 inch, note pad and pen (as per actual requirement) to each participant on the first day of course.



(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

(g) **Training Methodology:** The following training methodology will be followed by the institute: -

- (i) Training shall be conducted for 40 Hrs per week. The institute conducting training will devote 50% of total training towards the practical/ hands-on activities. In case additional classes are required, they can be planned for longer hours or on Saturdays.
- (ii) Training coverage shall be qualitative and exhaustive using audio and video tools. Power point slides will be used throughout the class.
- (iii) The classroom instruction must adhere strictly to the subject lesson plan, which should be prepared and approved well in advance of the course commencement. The lesson plan format is provided in **Appendix 'C'**. However bidders may modify the format with the buyer's written consent prior to the start of the course.
- (iv) Syllabus will be provided by bidder as per the SOR and approved by Depot IT, 11 BRD. The format of the syllabus is attached at **Appendix 'A'**. Any addition or deletion to it may be suggested by the institute and same may be incorporated, if agreed to.
- (v) Institute will prepare and submit detailed lesson plan (based on syllabus) as per attached format to the training monitoring committee for approval.
- (vi) Deviation from syllabus / lesson plan will be done after written approval by Depot IT, 11BRD
- (vii) Sufficient number of assignments will be given to participants.
- (viii) Two reference books as suggested by Training monitoring committee per course will be submitted to Depot IT along with course completion report.
- (ix) Two-time attendance (F/N & A/N) will be maintained for participants. The same will be submitted to Depot IT at the end of each course.
- (x) Institute will not grant leave to any participants. However, Depot IT may permit leave due to service exigencies or on compassionate ground.
- (xi) The institute will assist in all arrangements for conduct of the course like setting up the environment and administrative arrangements irrespective of the place of conduct of course.

(h) **Examination and Course Certification:**

- (i) For EC-Council Certification exam for Cyber Security courses and certification thereon to be facilitated and conducted by the institute. For this purpose, Institutes/Bidders are requested to quote the price separately, if any, as provisioned in Annexure III of the RFP (this price may or may not be included/considered in the standard price bid for the purpose of determining L1 bidder).

- (ii) For Full Stack Web Developer using Python Backend and Advance Hardware and Networking, the module test will be conducted at the end of each module. The institute will conduct re-test for participant those who fail in the module test, wherever required.
- (iii) The EC Council Certificate/ OEM certificates for all the respective course/ program with grades obtained shall be distributed by the institute to each participants.
- (iv) The trainees will be awarded grades as per attached **Appendix 'D'**.
- (j) **Feed Back:** To monitor the training regular feedback will be taken.
 - (i) The instructor will make attendance sheet as per the format given in **Appendix 'E'** for both the sessions-in the day
 - (ii) On first teaching day of each instructor, representatives of Depot IT will monitor the conduct of the class. The feedback of the same duly recommended by Depot IT Officer will be forwarded to institute in the format of the feedback as given at **Appendix 'F'**.
 - (iii) Course feedback will be taken from the Course leader to assess the conducted module. The format is given at **Appendix 'G'**
 - (iv) Feedback from the participants will be obtained from the participants verbally and feasible suggestions to be implemented by the institute accordingly.
 - (v) A course completion report will be submitted to the training monitoring committee within seven days of completion of each course. The course completion report will contain copies of screening and module mark sheet, feedbacks, lesson plan any other relevant information. The course completion report will be in bounded book form.
 - (vi) At the end of the course, consolidated feedback will be taken from the participants to assess the overall conduct of the course. The format is given at **Appendix 'H'**.
 - (vii) On completion of course, feedback on supply of courseware will be submitted by institute. Shortfalls, if any, are to be met within one week.
- (k) **Training Monitoring Committee:** - A training monitoring team will be constituted by the Depot IT 11 BRD, IAF that includes a representative from the institute and rest from Depot IT to monitor day-to-day progress of the courses. The name of the members of the team will be intimated to the institute.
- (l) **Cancellation of Course:** - The Depot IT Officer can cancel, postpone or reschedule any course to meet IAF exigency without mentioning a specific reason to the institute after the approval of competent authority.


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

(m) **Termination of Course**: Depot IT can terminate any ongoing course on recommendations of Training Monitoring Committee. The Depot IT Officer will give due consideration to feedback from participant after the approval of competent authority.

(n) **Termination of Contract**: If the contract is terminated for any reason, both parties will ensure that all ongoing commitments prior to the date of notice in relation to the Program already started and scheduled are complied with.

(o) **Dispute** - Disputes, if any between the two parties shall be settled by mutual negotiations between Executive Director of the institute and AOC, 11BRD. In case the amicable settlement is not arrived between them, the matter shall be referred to AOC-in-C HQ MC and his decision shall be final and binding on both the parties. Any lapses in conduct of the course are to be addressed at the level of Training monitoring committee and course coordinator in case of non-resolution of the same, the matter will be raised to the level of CP and AOC, 11BRD within one day of the occurrence.

(p) **Transfer of Duties** - The institute shall not assign or transfer any duties to any third parties

2. **Two Bid System**: This is a two-bid system and bidders are required to furnish clause by clause compliance of specifications bringing out clearly the deviation from specification, if any. The bidders are advised to submit clearly their compliance statements, in the format given in Annexure 'I' and Annexure 'II'.

3. **Training period**: The total training to be conducted as per the course scheduled enumerated in the contract, however, all the training to be completed within **Five months** from the date of acceptance of the contract. The contract may be extendable up to three years on same terms and conditions based on the previous year's performance of the institute

4. **Consignee details**: Depot IT Officer, 11 BRD, Airforce Station Ojhar, Nashik (MH).

5. **Inspection Authority**: Technical Team at Depot IT or their authorised rep.


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

PART III

STANDARD CONDITIONS OF RFP

1. The Bidder is also required to give confirmation of their acceptance of the under mentioned Standard Conditions of the Request for Proposal mentioned below which will automatically be considered as part of the Contract concluded with the successful Bidder (i.e. Seller in the Contract), as selected by the Buyer Failure to do so may result in rejection of the Bid submitted by the Bidder.
2. **Law:** The Contract shall be considered and made in accordance with the laws of the Republic of India. The Contract shall be governed by and interpreted in accordance with the laws of the Republic of India
3. **Effective Date of the Contract:** Normally the Contract shall come into effect on the date of signatures of both the parties on the Contract except when some other effective date is mutually agreed to and specifically indicated provided in the Contract. The deliveries and supplies and performances of the services shall commence from the effective date of the Contract.
4. **Arbitration:** All disputes or differences arising out of or in connection with the Contract shall be settled by bilateral discussions. Any dispute, disagreement or question arising out of or relating to the Contract or relating to construction or performance, which cannot be settled amicably, may be resolved through arbitration. The standard clause of arbitration is as per Forms DPM-7(for Private Indigenous Vendor), DPM-8(Foreign Vendors) and DPM-9 (CPSUS/DPSUs) (Available in MoD website <http://www.mod.nic.in>) The CFA will be the sole authority for appointment of sole arbitrator vide DPM-09 Para 711.1 The terms and clause as mentioned in the DPM 2009 will be applicable
5. **Penalty for use of Undue Influence:** The Seller undertakes that he has not given, offered or promised to give, directly or indirectly, any gift, consideration, reward, commission, fees, brokerage or inducement to any person in service of the Buyer or otherwise in procuring the Contracts or forbearing to do or for having done or forbome to do any act in relation to the obtaining or execution of the present Contract or any other Contract with the Government of India for showing or forbearing to show favor or disfavor to any person in relation to the present Contract or any other Contract with the Government of India. Any breach of the aforesaid undertaking by the Seller or any one employed by him or acting on his behalf (whether with or without the knowledge of the Seller) or the commission of any offers by the Seller or anyone employed by him or acting on his behalf, as defined in Chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act, 1988 or any other Act enacted for the prevention of corruption shall entitle the Buyer to cancel the Contract and all or any other Contracts with the Seller and recover from the Seller the amount of any loss arising from such cancellation. A decision of the Buyer or his nominee to the effect that a breach of the undertaking had been committed shall be final and binding on the Seller Giving or offering of any gift, bribe or inducement or any attempt at any such act on behalf of the Seller towards any officer/employee of the Buyer or to any other person in a position to influence any officer/employee of the Buyer for showing any favor in relation to this or any other Contract, shall render the Seller to such liability/ penalty as the Buyer may deem proper, including but not limited to termination of the Contract, imposition of penal damages, forfeiture of the Bank Guarantee and refund of the amounts paid by the Buyer.


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

6. **Agents/Agency Commission:** The Seller confirms and declares to the Buyer that the Seller is the original manufacturer of the stores/provider of the services referred to in this Contract and has not engaged any individual or firm, whether Indian or foreign whatsoever to intercede, facilitate or in any way to recommend to the Government of India or any of its functionaries, whether officially or unofficially, to the award of the Contract to the Seller nor has any amount been paid, promised or intended to be paid to any such individual or firm in respect of any such intercession, facilitation or recommendation. The Seller agrees that if it is established at any time to the satisfaction of the Buyer that the present declaration is in any way incorrect or if at a later stage it is discovered by the Buyer that the Seller has engaged any such individual/firm, and paid or intended to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution, whether before or after the signing of this Contract, the Seller will be liable to refund that amount to the Buyer. The Seller will also be debarred from entering into any Contract with the Government of India for a minimum period of five years. The Buyer will also have a right to consider cancellation of the Contract either wholly or in part, without any entitlement or compensation to the Seller who shall in such an event be liable to refund all payments made by the Buyer in terms of the Contract along with interest at the rate of 24% per annum above LIBOR rate. The Buyer will also have the right to recover any such amount from any Contracts concluded earlier with the Government of India

7. **Access to Books of Accounts:** In case it is found to the satisfaction of the Buyer that the Seller has engaged an Agent or paid commission or influenced any person to obtain the Contract as described in clauses relating to Agents/Agency Commission and penalty for use of undue influence, the Seller, on a specific request of the Buyer, shall provide necessary information/inspection of the relevant financial documents/information

8. **Non-disclosure of Contract documents:** Except with the written consent of the Buyer/Seller, other party shall not disclose the Contract or any provision, specification, plan, design, Pattern, sample or information thereof to any third party

9. **Liquidated Damages:** In the event of the Seller's failure to submit the Bonds, Guarantees and Documents, supply the stores/goods and conduct trials, installation of equipment, training etc. as specified in this Contract, the Buyer may, at his discretion, withhold any payment until the completion of the Contract. The BUYER may also deduct from the SELLER as agreed, liquidated damages to the sum of 0.5% of the Contract price of the delayed/undelivered stores/services mentioned above for every week of delay or part of a week, subject to the maximum value of the Liquidated Damages being not higher than 10% of the value of delayed stores

10. **Termination of Contract:** The Buyer shall have the right to terminate this Contract in Part or in full in any of the following cases.

- (a) The delivery of the material is delayed for causes not attributable to Force Majeure for more than (6 weeks) after the scheduled date of delivery.
- (b) The Seller is declared bankrupt or becomes insolvent
- (c) The delivery of material is delayed due to causes of Force Majeure by more than (1 months) provided Force Majeure clause is included in contract
- (d) The Buyer has noticed that the Seller has utilized the services of any Indian/Foreign agent in getting this contract and paid any commission to such individual/company etc.

- (e) As per decision of the Arbitration Tribunal.

11. **Notices:** Any notice required or permitted by the Contract shall be written in the English language and may be delivered personally or may be sent by FAX or registered pre-paid mail/airmail, addressed to the last known address of the party to whom it is sent.

12. **Transfer and Subletting:** The Seller has no right to give, bargain, sell, assign or sublet or otherwise dispose of the Contract or any part thereof, as well as to give or to let a third party take benefit or advantage of the present Contract or any part thereof.

13. **Patents and other Industrial Property Rights:** The prices stated in the present contract shall be deemed to include all amounts payable for the use of patents, copyrights, the prices stated in the present registered charges, trademarks and payments for any other industrial property rights. The Seller shall indemnify the Buyer against all claims from a third party at any time on account of the infringement of any or all the rights mentioned in the previous paragraphs, whether such claims arise in respect of manufacture or use. The Seller shall be responsible for the completion of the supplies including spares, tools, technical literature and training aggregates irrespective of the fact of infringement of the supplies, irrespective of the fact of infringement of any or all the rights mentioned above.

14. **Amendments:** No provision of present Contract shall be changed or modified in any way (including this provision) either in whole or in part except by an instrument in writing made after the date of this Contract and signed on behalf of both the parties and which expressly states to amend the present Contract.

15. **Taxes and Duties in respect of Indigenous Bidders**

(a) **General:**

(i) Bidders must indicate separately the relevant Taxes/Duties likely to be paid in connection with delivery of completed goods specified in RFP. In absence of this, the total cost quoted by them in their bids will be taken into account in the ranking of bids.

(ii) If a Bidder is exempted from payment of any duty/tax upto any value of supplies from them, he should clearly state that no such duty/tax will be charged by them up to the limit of exemption which they may have. If any concession is available in regard to rate/quantum of any Duty/tax, it should be brought out clearly. In such cases, relevant certificate will be issued by the Buyer later to enable the Seller to obtain exemptions from taxation authorities.

(iii) Any changes in levies, taxes and duties levied by Central/State/Local governments such as excise duty, VAT, Service tax, Octroi/entry tax, etc on final product upward as a result of any statutory variation taking place within contract period shall be allowed reimbursement by taking place within contract period shall be allowed reimbursement by the Buyer, to the extent of actual quantum of such duty/tax paid by the Seller. Similarly, in case of downward revision in any such duty/tax, the actual quantum of reduction of such duty/tax shall be reimbursed to the Buyer by the Seller. All such adjustments shall include all reliefs, exemptions, rebates, concession etc, if any,

obtained by the Seller Section 64-A of Sales of Goods Act will be relevant in this situation.

(iv) Levies, taxes and duties levied by Central/State/Local governments such as excise duty, VAT, Service tax, Octroi/entry tax, etc on final product will be paid by the Buyer on actuals based on relevant documentary evidence. Taxes and duties on input items will not be paid by Buyer and they may not be indicted separately in the bids. Bidders are required to include the same in the pricing of their product

(b) Customs Duty.

(i) In view of the amendment to exemption of Customs Duty issued vide Govt of India, Ministry of Finance vide notification No. 14/2016 dated 01 Mar 2016, CDEC will not be issued by the Buyer. Instead, the applicable Custom Duty as quoted in the commercial offer will be included in the contract and paid by the buyer. They will also indicate the rate of Custom Duty applicable along with the Indian Customs Tariff Numbers. Customs duty as actually paid will be reimbursed on production of necessary documents i.e.

(aa) Triplicate copy of the bill of entry,

(ab) copy of bill of lading,

(ac) a copy of foreign principal's invoice. However, if the Bidder imports the stores in question against his own commercial quota Import Licenses, he will also be required to submit in addition the triplicate copy of bills of entry etc. a certificate from his Internal Auditor on the bill itself, to the effect that the following items/quantity in the bill of entry related to the stores imported against Defense Buyer Supply Order number dated.

(ii) Subsequent to the reimbursement of customs duty, the Bidder will submit to the concerned Payment Authority a certificate to the effect that he has not obtained any refund of customs duty subsequent to the payment of duty to the Customs authority by him. In addition, he shall also submit to the Paying Authority concerned a certificate immediately after a period of three months from the date of payment of the duty to customs authorities to the effect that he has not applied for refund of the customs duty subsequent to the payment of duty to the customs authorities by him.

(iii) In case the Bidder obtains any refund of customs duty, subsequently to the payment of the same by him to the customs authorities and reimbursement of the customs duty to him by the Payment Authority, he should forthwith furnish the details of the refund obtained and afford full credit of the same to the Buyer.

(c) Excise Duty:

(i) Where the excise duty is payable on advalorem basis, the Bidder should submit along with the tender, the relevant form and the Manufacturer's price list showing the actual assessable value of the stores as approved by the Excise authorities.

(ii) Bidders should note that in case any refund of excise duty is granted to them by Excise authorities in respect of Stores supplied under the Contract, they will pass on the credit to the Buyer immediately along with a certificate that the credit so passed on relates to the Excise Duty, originally paid for the stores supplied under the Contract. In case of their failure to do so, within 10 days of the issue of the excise duty refund orders to them by the Excise Authorities the Buyer would be empowered to deduct a sum equivalent to the amount refunded by the Excise

Authorities without any further reference to them from any of their outstanding bills against the Contract or any other pending Government Contract and that no disputes on this account would be raised by them.

(iii) The Seller is also required to furnish to the Paying Authority the following certificates:

(aa) Certificate with each bill to the effect that no refund has been obtained in respect of the reimbursement of excise duty made to the Seller during three months immediately preceding the date of the claim covered by the relevant bill.

(ab) Certificate as to whether refunds have been obtained or applied for by them or not in the preceding financial year after the annual Audit of their accounts also indicating details of such refunds/applications, if any

(ac) A certificate along with the final payment bills of the Seller to the effect whether or not they have any pending appeal/protest for refund or partial refund of excise duties already reimbursed to the Seller by the Government pending with the Excise authorities and if so, the nature, the amount involved, and the position of such appeals

(ad) An undertaking to the effect that in case it is detected by the Government that any refund from Excise Authority was obtained by the Seller after obtaining reimbursement from the Paying Authority, and if the same is not immediately refunded by the Seller to the Paying Authority giving details and particulars of the transactions, Paying Authority will have full authority to recover such amounts from the Seller's outstanding bills against that particular Contract or any other pending Government Contracts and that no dispute on this account would be raised by the Seller.

(iv) Unless otherwise specifically agreed to in terms of the Contract, the Buyer shall not be liable for any claim on account of fresh imposition and/or increase of Excise Duty on raw materials and/or components used directly in the manufacture of the Contracted stores taking place during the pendency of the Contract.

(d) Sales Tax/GST

(i) If it is desired by the Bidder to ask for Sales tax/ GST to be paid as extra, the same must be specifically stated in the absence of any such stipulation in the bid, it will be presumed that the prices quoted by the Bidder are inclusive of sales tax and no liability of sales tax will be developed upon the Buyer.

(ii) On the Bids quoting sales tax extra, the rate and the nature of Sales Tax applicable at the time of supply should be shown separately Sales tax will be paid to the Seller at the rate at which it is liable to be assessed or has actually been assessed provided the transaction of sale is legally liable to sales tax and the same is payable as per the terms of the Contract.

(e) **Octroi Duty & Local Taxes**

(i) Normally, materials to be supplied to Government Departments against Government Contracts are exempted from levy of town duty, Octroi Duty, Terminal Tax and other levies of local bodies. The local Town/Municipal Body regulations at times, however, provide for such Exemption only on production of such exemption certificate from any authorised officer. Seller should ensure that stores ordered against Contracts placed by this office are exempted from levy of Town Duty/Octroi Duty, Terminal Tax or other local taxes and duties. Wherever required, they should obtain the exemption certificate from the Buyer, to avoid payment of such local taxes or duties.

(ii) In case where the Municipality or other local body insists upon payment of these duties or taxes the same should be paid by the Seller to avoid delay in supplies and possible demurrage charges. The receipt obtained for such payment should be forwarded to the Buyer without delay together with a copy of the relevant act or bylaws/ notifications of the Municipality of the local body concerned to enable him to take up the question of refund with the concerned bodies if admissible under the said acts or rules.


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

PART IV

SPECIAL CONDITIONS OF RFP

1. The Bidder is further required to give clause by clause confirmation of their acceptance of Special Conditions of the RFP mentioned below which will automatically be considered as part of the Contract concluded with the successful Bidder (i.e. Seller in the Supply Order) as selected by the Buyer. Failure to do so may result in rejection of Bid submitted by the Bidder

2. **Performance Security/Warranty/ Bank Guarantee:** Performance Security is payable by the successful bidder/supplier at the rate of 5% of the Supply Order value irrespective of the registration status of the firm. Performance Security deposit payable to the Purchaser is to be furnished by the Supplier in the form of a Performance Bank Guarantee (PBG) issued by a public sector bank or a private sector bank authorized to conduct government business, in the prescribed format within thirty days from the date of award of Supply Order. At present, ICICI Bank Ltd., Axis Bank Ltd. and HDFC Bank Ltd. are the three private sector banks authorized to carry out government transactions. The PBG/WBG will remain valid throughout the duration of the Contract Supply Order up-to completion of Contract and continue thereafter as a Warranty Bank Guarantee up to sixty days beyond the date of completion of all obligations of contract, including warranty on spares replaced/repared. This obviates the need to obtain a fresh Warranty/Bank Guarantee from the supplier on commencement of the warranty period, with corresponding return of the Performance Guarantee. In case the execution of the Supply Order is delayed beyond the Supply Ordered period and the purchaser grants extension of delivery period, with or without LD, the supplier must get the BG revalidated, if not already valid. The format of PBG cum WBG is given in Form DPM-15.

3. The Performance Bank Guarantee will be subject to encashment by the Buyer, in case the conditions regarding adherence to the delivery schedule, settlement of claims and other provisions of the Supply Order are not fulfilled by the Seller.

4. **Tolerance Clause** To take care of any change in the requirement during the period starting from issue of RFP till placement of the contract, Buyer reserves the right to $\pm 15\%$ increase or decrease the course strength up to that limit without any change in the terms & conditions and prices quoted by the Seller. While awarding the contract, the quantity ordered can be increased or decreased by the Buyer within this tolerance limit.

5. **Payment Terms:** It will be mandatory for the Bidders to submit ECS mandate and other relevant e-payment details so that payments could be made through ECS/EFT mechanism only. A copy of the model mandate form prescribed by RBI to be submitted by Bidders for receiving payments through ECS is available in MoD website and can be given on request. The payment will be made as per the following terms, on production of the requisite documents: -

(a) Payment will be made after completion of each course/batch as applicable subject to issuing of satisfactory report by Depot IT Officer.

(b) The similar payment schedule for three years will be applicable, if extended.

6. **Clarification of Technical/Course Related Matters:** Any clarification or enquiry(s) on course related matter shall be referred to Depot IT Officer, 11 BRD, AF.

7. **Advance Payments** No (R) No advance payment(s) will be made.

8. Paying Authority

(a) Senior Accounts Officer, 11BRD, Air Force Station Ojhar will be the paying authority for the payment of all bills on submission of the following documents by the Seller along with the bill:-

- (i) Ink-signed copy of contingent bill/Seller's bill
- (ii) Ink-signed copy of Commercial invoice/Seller's bill.
- (iii) Copy of Supply Order/Contract with U.O. number and date of IFA's concurrence, where required under delegation of powers.
- (iv) Claim for statutory and other levies to be supported with requisite documents / proof of payment such as Excise duty challan, Customs duty clearance certificate, Octroi receipt, proof of payment for EPF/ESIC contribution with nominal roll of beneficiaries, etc as applicable.
- (v) Exemption certificate for Taxes & duty, if applicable
- (vi) Bank guarantee for advance, if any.
- (vii) Performance Bank guarantee / Indemnity bond where applicable
- (viii) DP extension letter with CFA's sanction, U.O. number and date of IFA's concurrence, where required under delegation of powers, indicating whether extension is with or without LD
- (ix). Details for electronic payment viz Account holder's name, Bank name, Branch name and address, Account type, Account number, IFSC code, MICR code (if these details are not incorporated in supply order/contract)
- (x). Any other document/ certificate that may be provided for in the Supply Order/Contract
- (xi) Course completion certificate issued by Depot IT Officer, 11 BRD AF.

(b) Head of Account

MAJOR HEAD	2078
MINOR HEAD	110(L)
CODE HEAD	754/09

9. Fall Clause Seller is to confirm acceptance of fall clause as per provision of DPM 2009 covered in Pt-IV/Appendix 'C' of DPM 2009 (Page 188) which will form part of Supply Order. Fall Clause is applicable only for supplies to departments/organizations within India

- (a) The price charged for the stores supplied under the contract by the Seller shall in no event exceed the lowest prices at which the Seller sells the stores or offer to sell stores of identical description to any persons/Organization including the purchaser or any department of the Central government or any Department of state government or any statutory

undertaking the central or state government as the case may be during the period till performance of all supply Orders placed during the currency of the rate contract is completed

(b) If at any time, during the said period the Seller reduces the sale price, sells or offer to sell such stores to any person/organization including the Buyer or any Department of central Govt. or any Department of the State Government or any Statutory undertaking of the Central or state Government as the case may be at a price lower than the price chargeable under the contract, the shall forthwith notify such reduction or sale or offer of sale to the Director general of Supplies & Disposals and the price payable under the contract for the stores of such reduction of sale or offer of the sale shall stand correspondingly reduced. The above stipulation will, however, not apply to-

(i) Exports by the Seller

(ii) Sale of goods as original equipment at price lower than lower than the prices charged for normal replacement

(iii) Sale of goods such as drugs which have expiry dates.

(iv) Sale of goods at lower price on or after the date of completion of sale/placement of the order of goods by the authority concerned under the existing or previous Rate Contracts as also under any previous contracts entered into with the Central or State Govt. Depts, including their undertakings excluding joint sector companies and/or private parties and bodies

10. **Specification:** As per Schedule of Requirement placed at **Part-II Para 1** of RFP.

11. **Franking clause:** The following Franking clause will form part of the contract placed on successful Bidder –

(a) **Franking Clause in the case of Acceptance of Goods.** "The fact that the goods have been inspected after the delivery period and passed by the Inspecting Officer will not have the effect of keeping the contract alive. The goods are being passed without prejudice to the rights of the Buyer under the terms and conditions of the contract"

(b) **Franking Clause in the case of Rejection of Goods.** "The fact that the goods have been inspected after the delivery period and rejected by the Inspecting Officer will not bind the Buyer in any manner. The goods are being rejected without prejudice to the rights of the Buyer under the terms and conditions of the contract"

12. **Force Majeure Clause:-**

(a) Neither party shall bear responsibility for the complete or partial non-performance of any of its obligations (except for failure to pay any sum which has become due on account of receipt of goods under the provisions of the present contract), if the non- performance results from such Force Majeure circumstances as Flood, Fire, earthquake and other acts of God as well as War, Military operation, blockade, Acts or Actions of State Authorities or any other circumstances beyond the parties control that have arisen after the conclusion of the present contract

(b) In such circumstances the time stipulated for the performance of an obligation under the present contract is extended correspondingly for the period of time of action of these circumstances and their consequences.

(c) The party for which it becomes impossible to meet obligations under this contract due to Force Majeure conditions, is to notify in written form the other party of the beginning and cessation of the above circumstances immediately, but in any case not later than ten days from the moment of their beginning.

(d) Certificate of a Chamber of Commerce (Commerce and Industry) or other competent authority or organization of the respective country shall be a sufficient proof of commencement and cessation of the above circumstances.

(e) If the impossibility of complete or partial performance of an obligation lasts for more than six months, either party hereto reserves the right to terminate the contract totally or partially upon giving prior written notice of 30 (thirty) days to the other party of the intention to terminate without any liability other than reimbursement on the terms provided in the agreement for the goods received.



(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

PART V

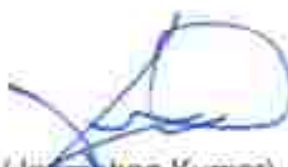
EVALUATION CRITERIA & PRICE BID ISSUES

1. **Evaluation Criteria**:- The broad guidelines for evaluation of Bids will be as follows:-
 - (a) Only those Bids will be evaluated which are found to be fulfilling all the eligibility and qualifying requirements of the RFP, both technically and commercially.
 - (b) Priority will be given to Govt. aided institutions.
 - (c) The Comprehensive Lowest Acceptable Bid will be decided on the basis of consolidated price for all the courses quoted by the particular Bidder as per the Price Format provided in BOQ.xls or Format given in Annexure 'III' of the RFP along with tender documents.
 - (d) If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price will prevail and the total price will be corrected if there is a discrepancy between words and figures; the amount in words will prevail for calculation of price.
 - (f) The Comprehensive Lowest Acceptable Bid will be considered further for placement of contract / Supply Order after complete clarification and price negotiations as decided by the Buyer. The Buyer also reserves the right to do Apportionment of Quantity, if it is convinced that Lowest Bidder is not in a position to supply full quantity in stipulated time.
2. **Technical Bid Format**: The Technical Bid Format should be as per attached Performa (Annexure 'I') and Bidders are required to fill this up correctly with full details. Firms are required to submit full details on separate sheets wherever applicable such as Man hour's detail/Bill of materials etc.
3. **Financial/Commercial Bid Performa**:- The Commercial bid format is provided as BoQ.xls or Format given in Annexure 'III' of the RFP along with this tender document at <https://eprocure.gov.in/eprocure/app> Bidders are advised to download this BoQ.xls as it is, and quote their offer in the permitted column. Bidders are also to fill the duties & Taxes columns as applicable, to ascertain the total cash outgo. However, the determination of L-1 will be done as per the above-mentioned evaluation criteria. **Bidders must quote for the EC-Council Certification exam Fee for Cyber Security courses and certification, failing which leads to rejection / invalidation of Bid.**
4. **Tender Acceptance Certificate**: An Undertaking/ Tender Acceptance certificate (as per Annexure IV), duly filled complete in all respects, should also be submitted by Institutes / firm along with their technical bids Please confirm that the services offered by you is exactly as required under tender enquiry description specification.


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

Sl No.	Course Name	No of Participants	No of Courses	Course Duration
1.	Cyber Security Courses :-			
	(a) Certified Ethical Hacker (CEH v12)	20	01	2 Weeks
	(b) Certified Threat Intelligence Analyst (CTIA)	20	01	2 Weeks
	(c) Computer Hacking Forensic Investigator (CHFI)	20	01	2 Weeks
	(d) Certified Penetration Testing (CPENT)	20	01	2 Weeks
	(e) Certified Application Security Engineer (CASE)	20	01	2 Weeks
2.	Full Stack Web Developer Using Python	20	01	4 Weeks
3.	Advanced Hardware and Networking	20	02	2 Weeks

Note:- This RFP is being issued with no financial commitment and the Buyer reserves the right to change or vary any part thereof at any stage. Buyer also reserves the right to withdraw the RFP, should it become necessary at any stage.



(Jagmohan Kumar)
Wing Commander
Depot IT Officer
For Air Officer Commanding

Appendix: As stated.
Annexure 'I': Technical Bid Performance.
Annexure 'II': Certificates to be submitted along with the Technical bid
Annexure 'III': Financial/Commercial Bid Performance.
Annexure 'IV': Tender Acceptance Letter/Certificate



(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

Check List for Bidders

Envelope	Document	Reference
Envelope 1 (Technical Bid)	EMD	Refers to Part- I Para 4 (a) & Part- I Para 16 of the RFP
	Technical Bid Performa	Annexure-'I' of RFP
	Documents/Certificates	As per Annexure-'II' of RFP
	Tender Acceptance Letter/Certificate	Annexure-'IV' of RFP
Envelope 2 (Commercial Bid)	Commercial / Financial Bid Performa	Annexure-'III' of RFP


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

DETAILS OF IT TRAINING COURSES

SI No.	Course Name	No of Participants	No of Courses	Course Duration
1.	Cyber Security Courses :-			
	(a) Certified Ethical Hacker (CEH v12)	20	01	2 Weeks
	(b) Certified Threat Intelligence Analyst (CTIA)	20	01	2 Weeks
	(c) Computer Hacking Forensic Investigator (CHFI)	20	01	2 Weeks
	(d) Certified Penetration Testing (CPENT)	20	01	2 Weeks
	(e) Certified Application Security Engineer (CASE)	20	01	2 Weeks
2.	Advanced Web Designing/Full Stack Web Developer Using Python	20	01	4 Weeks
3.	Advanced Hardware and Networking	20	02	2 Weeks


(Jagmohan Kumar)
Wg Cdr
Depot IT Officer

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

1. TRAINING OF CYBER SECURITY COURSE

(a) COURSE: CERTIFIED ETHICAL HACKER (CEH v12)

Course Overview

This 100-hour course is designed to provide a comprehensive understanding of ethical hacking methodologies, tools, and techniques. It aligns with the CEH v12 exam objectives, emphasizing a 50/50 balance between theoretical knowledge and practical application.

Course Structure

The course is divided into 20 modules, each focusing on a specific area of ethical hacking.

Module 1: Introduction to Ethical Hacking (5 hours)

- **Theory (2.5 hours):**
 - Ethical hacking vs. cracking
 - Legal and ethical considerations
 - The hacking lifecycle
 - Information security concepts
- **Practice (2.5 hours):**
 - Ethical hacking policy creation
 - Risk assessment and management

Module 2: Footprinting and Reconnaissance (5 hours)

- **Theory (2.5 hours):**
 - Footprinting techniques (whois, DNS, social media)
 - Reconnaissance techniques (banner grabbing, directory busting)
 - Open-source intelligence (OSINT)
- **Practice (2.5 hours):**
 - Foot printing and reconnaissance exercises using tools like Shodan, Google Dorks, Maltego
 - OSINT gathering

Module 3: Scanning Networks (5 hours)

- **Theory (2.5 hours):**
 - Network scanning tools (Nmap, Nessus)

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- Port scanning techniques
- Vulnerability scanning
- **Practice (2.5 hours):**
 - Network scanning exercises using Nmap, Nessus
 - Vulnerability assessment using Nessus

Module 4: Enumeration (5 hours)

- **Theory (2.5 hours):**
 - Enumeration techniques (user enumeration, share enumeration)
 - Active and passive enumeration
 - Post-exploitation enumeration
- **Practice (2.5 hours):**
 - Enumeration exercises using tools like Metasploit, Burp Suite
 - Information gathering from target systems

Module 5: Vulnerability Analysis (5 hours)

- **Theory (2.5 hours):**
 - Vulnerability assessment methodologies
 - Vulnerability scanning tools
 - Risk assessment
- **Practice (2.5 hours):**
 - Vulnerability scanning and analysis using Nessus, OpenVAS
 - Risk assessment and prioritization

Module 6: System Hacking (5 hours)

- **Theory (2.5 hours):**
 - System hacking techniques (password cracking, keylogging)
 - Privilege escalation
 - Backdoors and rootkits
- **Practice (2.5 hours):**
 - Password cracking exercises using tools like John the Ripper, Hashcat
 - Privilege escalation challenges in vulnerable systems
 - Rootkit detection using tools like chkrootkit

Module 7: Malware Threats (5 hours)

- **Theory (2.5 hours):**

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 08 DEC 24

- Malware types (viruses, worms, trojans)
- Malware delivery methods
- Malware analysis techniques
- **Practice (2.5 hours):**
 - Malware analysis using tools like IDA Pro, Ghidra
 - Malware prevention and detection using antivirus software

Module 8: Sniffing (5 hours)

- **Theory (2.5 hours):**
 - Sniffing techniques and tools (Wireshark)
 - Protocol analysis
 - Countermeasures
- **Practice (2.5 hours):**
 - Packet capture and analysis using Wireshark
 - Sniffing attacks and defenses

Module 9: Social Engineering (5 hours)

- **Theory (2.5 hours):**
 - Social engineering tactics (phishing, pretexting)
 - Human psychology in security
 - Countermeasures
- **Practice (2.5 hours):**
 - Social engineering simulations (email phishing, phone phishing)
 - Awareness training

Module 10: Denial-of-Service (5 hours)

- **Theory (2.5 hours):**
 - DoS and DDoS attacks
 - Attack vectors
 - Mitigation techniques
- **Practice (2.5 hours):**
 - DoS/DDoS attack simulations using tools like Hping3, Low Orbit Ion Cannon
 - DDoS mitigation techniques

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

Module 11: Session Hijacking (5 hours)

- **Theory (2.5 hours):**
 - Session management concepts
 - Session hijacking techniques (cookie poisoning, session fixation)
 - Countermeasures (HTTPS, session timeouts)
- **Practice (2.5 hours):**
 - Session hijacking attacks using tools like Burp Suite
 - Implementing secure session management practices

Module 12: Evading IDS, Firewalls, and Honeypots (5 hours)

- **Theory (2.5 hours):**
 - IDS/IPS evasion techniques
 - Firewall bypassing methods
 - Honeypot detection
- **Practice (2.5 hours):**
 - IDS/IPS evasion testing
 - Firewall bypassing challenges
 - Honeypot detection and exploitation

Module 13: Hacking Web Servers (5 hours)

- **Theory (2.5 hours):**
 - Web server vulnerabilities (directory traversal, file inclusion)
 - Web server attacks (HTTP flooding, brute force)
 - Countermeasures (web application firewalls, intrusion detection)
- **Practice (2.5 hours):**
 - Web server vulnerability scanning using tools like Nessus
 - Web server attack simulations
 - Web server hardening

Module 14: Hacking Web Applications (5 hours)

- **Theory (2.5 hours):**
 - Web application vulnerabilities (SQL injection, cross-site scripting)
 - Web application attacks (session hijacking, cross-site request forgery)
 - Countermeasures (input validation, output encoding)

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- **Practice (2.5 hours):**

- Web application vulnerability scanning using tools like Burp Suite
- Web application penetration testing
- Secure coding practices

Module 15: SQL Injection (5 hours)

- **Theory (2.5 hours):**

- SQL injection types (blind, error-based)
- SQL injection prevention
- Countermeasures (parameterized queries, stored procedures)

- **Practice (2.5 hours):**

- SQL injection attacks
- SQL injection prevention and detection

Module 16: Hacking Wireless Networks (5 hours)

- **Theory (2.5 hours):**

- Wireless network vulnerabilities (WEP, WPA, WPS)
- Wireless hacking techniques (war driving, cracking)
- Countermeasures (WPA2, strong passwords)

- **Practice (2.5 hours):**

- Wi-Fi auditing using tools like Aircrack-ng
- Wireless network cracking
- Wireless network security best practices

Module 17: Hacking Mobile Platforms (5 hours)

- **Theory (2.5 hours):**

- Mobile platform vulnerabilities (Android, iOS)
- Mobile application security
- Mobile device management

- **Practice (2.5 hours):**

- Mobile application testing for vulnerabilities
- Mobile device forensics
- Mobile security best practices

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

Module 18: IoT Hacking (5 hours)

- **Theory (2.5 hours):**
 - IoT security challenges
 - IoT attack vectors
 - IoT security best practices
- **Practice (2.5 hours):**
 - IoT device vulnerability assessment
 - IoT device hacking
 - IoT security hardening

Module 19: Cloud Computing (5 hours)

- **Theory (2.5 hours):**
 - Cloud security models
 - Cloud threats and vulnerabilities
 - Cloud security best practices
- **Practice (2.5 hours):**
 - Cloud security assessment
 - Cloud penetration testing
 - Cloud security configuration

Module 20: Cryptography (5 hours)

- **Theory (2.5 hours):**
 - Cryptographic algorithms (symmetric, asymmetric)
 - Cryptographic protocols (TLS, SSL)
 - Cryptographic attacks
- **Practice (2.5 hours):**
 - Cryptography implementation and testing
 - Cryptography attacks and defences

SCHEDULE OF REQUIREMENT
11BRD/4724/1/T BM-II DATED 06 DEC 24

(b) COURSE: CERTIFIED THREAT INTELLIGENCE ANALYST (C/TIA)

Course Overview

This 100-hour course is designed to provide a comprehensive understanding of threat intelligence, enabling students to effectively collect, analyse, and disseminate actionable intelligence to protect organizations from cyber threats. The curriculum emphasizes a 50/50 balance between theoretical knowledge and practical application.

Course Structure

The course is divided into eight modules, each focusing on a specific aspect of threat intelligence.

Module 1: Introduction to Threat Intelligence (5 hours)

- **Theory (2.5 hours):**
 - Definition and importance of threat intelligence
 - Threat intelligence lifecycle
 - Threat intelligence frameworks (Diamond Model, Kill Chain)
 - Threat intelligence value chain
- **Practice (2.5 hours):**
 - Threat intelligence use case scenarios
 - Threat intelligence platform overview

Module 2: Cyber Threats and Attack Frameworks (10 hours)

- **Theory (5 hours):**
 - Types of cyber threats (APT, malware, Ransomware, etc.)
 - Attack methodologies (MITRE ATT&CK, Cyber Kill Chain)
 - Threat actor profiles
 - Indicators of compromise (IOCs)
- **Practice (5 hours):**
 - Threat actor profiling exercises
 - IOC analysis and correlation

Module 3: Requirements, Planning, Direction, and Review (5 hours)

- **Theory (2.5 hours):**
 - Threat intelligence program development
 - Stakeholder management

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- Threat intelligence requirements gathering
- Measuring threat intelligence effectiveness
- **Practice (2.5 hours):**
 - Developing a threat intelligence program roadmap
 - Threat intelligence metrics and KPIs

Module 4: Data Collection and Processing (10 hours)

- **Theory (5 hours):**
 - Data sources (open-source, proprietary, internal)
 - Data collection techniques (scraping, APIs, sensors)
 - Data enrichment and normalization
 - Data quality and governance
- **Practice (5 hours):**
 - Data collection using open-source intelligence tools
 - Data enrichment and normalization using scripting languages

Module 5: Data Analysis (15 hours)

- **Theory (7.5 hours):**
 - Threat intelligence analysis techniques (STIX, TAXII)
 - Data visualization and storytelling
 - Correlation and attribution
 - Predictive analytics
- **Practice (7.5 hours):**
 - Threat intelligence analysis using threat intelligence platforms
 - Data visualization and reporting
 - Correlation and attribution exercises

Module 6: Intelligence Reporting and Dissemination (5 hours)

- **Theory (2.5 hours):**
 - Threat intelligence report formats
 - Effective communication of intelligence
 - Intelligence dissemination channels
- **Practice (2.5 hours):**
 - Creating threat intelligence reports
 - Tailoring intelligence for different audiences

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

Module 7: Threat Hunting and Detection (10 hours)

- **Theory (5 hours):**
 - Threat hunting concepts
 - Threat hunting methodologies
 - Integration with security operations
- **Practice (5 hours):**
 - Threat hunting simulations
 - Incident response planning

Module 8: Threat Intelligence in SOC Operations, Incident Response, and Risk Management (5 hours)

- **Theory (2.5 hours):**
 - Threat intelligence integration with SOC
 - Threat intelligence for incident response
 - Threat intelligence for risk management
- **Practice (2.5 hours):**
 - Threat intelligence-driven incident response simulation
 - Risk assessment using threat intelligence

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

(c) COURSE: CERTIFIED HACKING FORENSIC INVESTIGATOR (C(HFI) V11

Course Overview

This 100-hour course is designed to provide a comprehensive understanding of digital forensics, equipping students with the knowledge and skills to conduct thorough investigations and analyse digital evidence effectively. The curriculum is structured with a 50/50 balance of theoretical knowledge and practical application.

Course Structure

The course is divided into 15 modules, each focusing on a specific area of digital forensics.

Module 1: Computer Forensics in Today's World (5 hours)

- **Theory (2.5 hours):**
 - Introduction to digital forensics
 - The role of a digital forensic investigator
 - Legal and ethical considerations
 - The digital forensic process
- **Practice (2.5 hours):**
 - Case studies of high-profile digital forensics cases
 - Ethical hacking scenarios and forensic response

Module 2: Computer Forensics Investigation Process (5 hours)

- **Theory (2.5 hours):**
 - The digital forensic investigation process
 - Evidence collection and preservation
 - Chain of custody
 - Forensic tools and software
- **Practice (2.5 hours):**
 - Creating a forensic investigation plan
 - Documenting evidence collection and chain of custody

Module 3: Understanding Hard Disks and File Systems (5 hours)

- **Theory (2.5 hours):**
 - Hard disk anatomy
 - File system structures (FAT, NTFS, ext2/3/4)
 - Data recovery concepts

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- **Practice (2.5 hours):**

- Disk imaging and analysis
- File system exploration using forensic tools

Module 4: Data Acquisition and Duplication (5 hours)

- **Theory (2.5 hours):**

- Data acquisition methods (live, static)
- Data duplication techniques
- Forensic imaging standards

- **Practice (2.5 hours):**

- Performing live and static acquisitions
- Creating forensic images
- Verifying image integrity

Module 5: Defeating Anti-Forensics Techniques (5 hours)

- **Theory (2.5 hours):**

- Anti-forensics methods (data wiping, encryption, steganography)
- Countermeasures and detection techniques

- **Practice (2.5 hours):**

- Analyzing data with anti-forensics techniques applied
- Developing countermeasures

Module 6: Windows Forensics (10 hours)

- **Theory (5 hours):**

- Windows file system structure
- Registry analysis
- Windows artifacts

- **Practice (5 hours):**

- Analyzing Windows systems
- Recovering deleted files
- Investigating Windows-based crimes

Module 7: Linux and Mac Forensics (5 hours)

- **Theory (2.5 hours):**

- Linux and Mac file system structures

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- Linux and Mac artifacts
- Cross-platform forensics
- **Practice (2.5 hours):**
 - Analyzing Linux and Mac systems
 - Recovering data from Linux and Mac systems

Module 8: Network Forensics (5 hours)

- **Theory (2.5 hours):**
 - Network forensics concepts
 - Network traffic analysis
 - Digital evidence in network communications
- **Practice (2.5 hours):**
 - Network packet capture and analysis
 - Investigating network-based crimes

Module 9: Malware Forensics (5 hours)

- **Theory (2.5 hours):**
 - Malware types and behaviours
 - Malware analysis techniques
 - Malware incident response
- **Practice (2.5 hours):**
 - Malware analysis using sandboxes
 - Investigating malware infections

Module 10: Investigating Web Attacks (5 hours)

- **Theory (2.5 hours):**
 - Web application attacks
 - Web server forensics
 - Digital evidence in web attacks
- **Practice (2.5 hours):**
 - Investigating web server logs
 - Analyzing web application vulnerabilities

Module 11: Dark Web Forensics (5 hours)

- **Theory (2.5 hours):**

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- The dark web and its role in crime
- Investigating dark web activities
- Challenges in dark web forensics
- **Practice (2.5 hours):**
 - Using dark web search engines and marketplaces
 - Analyzing dark web data
 - Identifying potential criminal activity

Module 12: Cloud Forensics (5 hours)

- **Theory (2.5 hours):**
 - Cloud computing and forensic challenges
 - Cloud data acquisition and preservation
 - Cloud-based investigations
- **Practice (2.5 hours):**
 - Cloud forensics tools and techniques
 - Investigating cloud-based incidents

Module 13: Email and Social Media Forensics (5 hours)

- **Theory (2.5 hours):**
 - Email and social media as evidence sources
 - Email header analysis
 - Social media data collection and analysis
- **Practice (2.5 hours):**
 - Email forensics analysis and Social media investigations

Module 14: Mobile Forensics (10 hours)

- **Theory (5 hours):**
 - Mobile device architecture
 - Mobile operating systems (iOS, Android)
 - Mobile data extraction and analysis
- **Practice (5 hours):**
 - Mobile device acquisition
 - Mobile data analysis using forensic tools
 - Mobile application forensics

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

Module 15: IoT Forensics (5 hours)

- **Theory (2.5 hours):**
 - IoT devices and their forensic challenges
 - IoT data acquisition and analysis
 - IoT incident response
- **Practice (2.5 hours):**
 - IoT device forensics
 - IoT data extraction and analysis

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

(d) COURSE: CERTIFIED PENETRATION TESTING PROFESSIONAL (C|PENT)

Course Overview

This 100-hour course is designed to provide a comprehensive understanding of penetration testing methodologies, tools, and techniques. It aligns with the C|PENT exam objectives, emphasizing a 50/50 balance between theoretical knowledge and practical application.

Course Structure

The course is divided into 14 modules, each focusing on a specific area of penetration testing.

Module 1: Introduction to Penetration Testing and Methodologies (5 hours)

- **Theory (2.5 hours):**
 - Definition of penetration testing
 - Penetration testing methodologies (black box, white box, grey box)
 - Legal and ethical considerations
 - Relationship to other security disciplines
- **Practice (2.5 hours):**
 - Ethical hacking policy creation
 - Risk assessment and management

Module 2: Penetration Testing Scoping and Engagement (5 hours)

- **Theory (2.5 hours):**
 - Penetration testing lifecycle
 - Scoping and planning
 - Contract negotiation
 - Communication with clients
- **Practice (2.5 hours):**
 - Creating penetration testing project plans
 - Developing engagement contracts

Module 3: Open-Source Intelligence (OSINT) (5 hours)

- **Theory (2.5 hours):**
 - OSINT techniques and tools
 - Social media intelligence

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- Dark web research
- **Practice (2.5 hours):**
 - Conducting OSINT investigations on target organizations
 - Building intelligence reports

Module 4: Social Engineering Penetration Testing (5 hours)

- **Theory (2.5 hours):**
 - Social engineering principles
 - Attack vectors (phishing, pretexting, baiting)
 - Countermeasures
- **Practice (2.5 hours):**
 - Social engineering simulations
 - Awareness training

Module 5: Network Penetration Testing – External (10 hours)

- **Theory (5 hours):**
 - Network reconnaissance
 - Vulnerability scanning
 - Exploitation
 - Post-exploitation
- **Practice (5 hours):**
 - External penetration testing using tools like Nmap, Metasploit
 - Exploitation of vulnerabilities

Module 6: Network Penetration Testing – Internal (10 hours)

- **Theory (5 hours):**
 - Internal network assessment
 - Active directory exploitation
 - Lateral movement
 - Privilege escalation
- **Practice (5 hours):**
 - Internal penetration testing simulations
 - Active directory exploitation

Module 7: Network Penetration Testing - Perimeter Devices (5 hours)

- **Theory (2.5 hours):**

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- Perimeter device vulnerabilities
- Firewall testing
- IDS/IPS evasion

- **Practice (2.5 hours):**

- Firewall testing and bypassing
- IDS/IPS evasion techniques

Module 8: Web Application Penetration Testing (10 hours)

- **Theory (5 hours):**

- Web application vulnerabilities (OWASP Top 10)
- Web application attack methodologies
- Web application security testing tools

- **Practice (5 hours):**

- Web application penetration testing using Burp Suite
- Exploiting web application vulnerabilities

Module 9: Wireless Penetration Testing (5 hours)

- **Theory (2.5 hours):**

- Wireless network fundamentals
- Wireless security protocols (WEP, WPA, WPA2)
- Wireless attack methodologies (war driving, cracking)
- Countermeasures

- **Practice (2.5 hours):**

- Wireless network auditing using tools like Aircrack-ng
- Wireless network cracking
- Wireless network security best practices

Module 10: IoT Penetration Testing (5 hours)

- **Theory (2.5 hours):**

- IoT device vulnerabilities
- IoT attack surface
- IoT security testing methodologies

- **Practice (2.5 hours):**

- IoT device reconnaissance
- IoT device hacking

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- IoT security assessment

Module 11: OT and SCADA Penetration Testing (5 hours)

- **Theory (2.5 hours):**
 - OT and SCADA system overview
 - OT and SCADA security risks
 - Penetration testing methodologies for OT/SCADA
- **Practice (2.5 hours):**
 - OT/SCADA network reconnaissance
 - OT/SCADA system vulnerability assessment
 - OT/SCADA incident response simulation

Module 12: Cloud Penetration Testing (5 hours)

- **Theory (2.5 hours):**
 - Cloud security models
 - Cloud-based threats and vulnerabilities
 - Cloud penetration testing methodologies
- **Practice (2.5 hours):**
 - Cloud infrastructure assessment
 - Cloud application penetration testing
 - Cloud data security testing

Module 13: Binary Analysis and Exploitation (5 hours)

- **Theory (2.5 hours):**
 - Reverse engineering concepts
 - Binary analysis techniques
 - Exploit development
- **Practice (2.5 hours):**
 - Binary analysis using tools like IDA Pro, Ghidra
 - Exploit development

Module 14: Report Writing and Post Testing Actions (5 hours)

- **Theory (2.5 hours):**
 - Penetration testing report structure
 - Vulnerability assessment and risk rating
 - Remediation recommendations

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- **Practice (2.5 hours):**
 - Creating penetration testing reports
 - Developing remediation plans

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

(e) COURSE: CERTIFIED APPLICATION SECURITY ENGINEER

Course Overview

This 100-hour course is designed to equip participants with the knowledge and skills necessary to become Certified Application Security Engineers. The curriculum is structured with a balanced approach of 50% theory and 50% practical exercises to ensure a comprehensive understanding of application security principles and their application in real-world scenarios.

Course Structure

The course is divided into ten modules, each focusing on a specific aspect of application security.

Module 1: Understanding Application Security, Threats, and Attacks (10 hours)

- **Theory (5 hours):**
 - Definition of application security
 - The OWASP Top 10 and other threat classifications
 - Attack vectors (injection, cross-site scripting, SQL injection, etc.)
 - Impact of vulnerabilities on organizations
- **Practice (5 hours):**
 - Hands-on exercises on vulnerability identification
 - Threat modeling workshops
 - Case studies of real-world attacks

Module 2: Security Requirements Gathering (5 hours)

- **Theory (2.5 hours):**
 - Importance of security requirements
 - Threat modeling techniques (STRIDE, OCTAVE, etc.)
 - Risk assessment methodologies
- **Practice (2.5 hours):**
 - Conducting threat modeling exercises
 - Risk assessment workshops
 - Creating security requirements documents

Module 3: Secure Application Design and Architecture (10 hours)

- **Theory (5 hours):**
 - Security by design principles

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- Secure architecture patterns
- Defense-in-depth strategies

- **Practice (5 hours):**

- Designing secure architectures
- Code review for security vulnerabilities
- Architectural risk analysis

Module 4: Secure Coding Practices for Input Validation (10 hours)

- **Theory (5 hours):**

- Input validation techniques
- Preventing injection attacks
- Handling sensitive data

- **Practice (5 hours):**

- Coding exercises with input validation
- Code review for input validation flaws
- Vulnerability testing for input validation

Module 5: Secure Coding Practices for Authentication and Authorization (10 hours)

- **Theory (5 hours):**

- Authentication mechanisms (password-based, token-based, biometric)
- Authorization models (role-based, attribute-based)
- Secure session management

- **Practice (5 hours):**

- Implementing authentication and authorization
- Session management testing
- Vulnerability assessment for authentication and authorization

Module 6: Secure Coding Practices for Cryptography (10 hours)

- **Theory (5 hours):**

- Cryptographic algorithms and key management
- Secure key storage and distribution
- Data encryption and decryption

- **Practice (5 hours):**

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- Cryptography implementation exercises
- Cryptographic key management practices
- Cryptographic vulnerability assessment

Module 7: Secure Coding Practices for Session Management (5 hours)

- **Theory (2.5 hours):**

- Session management concepts
- Session hijacking prevention
- Session timeout and expiration

- **Practice (2.5 hours):**

- Implementing secure session management
- Session management testing
- Vulnerability assessment for session management

Module 8: Secure Coding Practices for Error Handling (5 hours)

- **Theory (2.5 hours):**

- Error handling best practices
- Preventing information leakage
- Handling exceptions gracefully

- **Practice (2.5 hours):**

- Error handling code implementation
- Error handling testing
- Vulnerability assessment for error handling

Module 9: Static and Dynamic Application Security Testing (SAST & DAST) (10 hours)

- **Theory (5 hours):**

- SAST and DAST concepts
- False positives and false negatives
- Integration of SAST and DAST

- **Practice (5 hours):**

- Hands-on SAST and DAST tool usage
- Vulnerability scanning and remediation
- SAST and DAST report analysis

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

Module 10: Secure Deployment and Maintenance (10 hours)

- **Theory (5 hours):**
 - Secure deployment practices
 - Vulnerability management
 - Incident response planning
- **Practice (5 hours):**
 - Deployment security checklist
 - Vulnerability scanning and patching
 - Incident response simulation

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

3. COURSE: FULL STACK WEB DEVELOPMENT COURSE (PYTHON BACKEND) WITH SHAREPOINT

Course Overview

This 200-hour course is designed to equip participants with the knowledge and skills necessary to become a full-stack web developer, focusing on Python for back-end development. You'll learn to build dynamic and interactive web applications from scratch, mastering both front-end and back-end technologies. The curriculum is structured with a balanced approach of 50% theory and 50% practical exercises to ensure a comprehensive understanding of application security principles and their application in real-world scenarios.

Course Structure:

The course is divided into 14 modules (08-Python backend & 08-MS SharePoint), with hands-on labs, projects, and assignments integrated throughout the program additionally this course integrated with Microsoft SharePoint which enhance the knowledge of working professional.

PART-I

(FULL STACK WEB DEVELOPMENT COURSE (PYTHON BACKEND))

Module 1: Front-End Development Fundamentals (30 Hrs)

- o Introduction to HTML5
- o Cascading Style Sheets (CSS3)
- o Responsive Web Design (RWD)
- o JavaScript Fundamentals
- o DOM Manipulation

Module 2: Advanced Front-End Development (35 Hrs)

- o JavaScript Frameworks (Choose One)
- o Component-Based Architecture
- o Front-End Build Tools
- o Client-Side Routing
- o APIs and AJAX

Module 3: Python Programming Fundamentals (30 Hrs)

- o Introduction to Python
- o Data Structures and Algorithms
- o Version Control with Git
- o Testing with Python Libraries
- o Debugging Techniques

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

Module 4: Python for Back-End Development (35 Hrs)

- o Web Frameworks with Python (Focus on Django)
- o Databases with Python
- o Object-Relational Mappers (ORMs)
- o User Authentication and Authorization
- o RESTful API Development with Django REST framework

Module 5: Full-Stack Integration and Deployment (20 Hrs)

- o Front-End and Back-End Communication
- o Security Best Practices
- o Deployment Strategies
- o Server Administration Fundamentals:
- o (CI/CD)

Module 6: Project Development (on Saturday/Weekend)

- o Full-Stack Project Development

PART-II

MICROSOFT SHAREPOINT 19 COURSE OUTLINE

Module 1: Introduction to SharePoint 19 (02 Hrs)

- o Overview of SharePoint 19 (Online & On-Premises)
- o Key benefits and use cases of SharePoint
- o Understanding the SharePoint architecture
- o Exploring the modern and classic SharePoint experiences

Module 2: Navigating SharePoint 19 (03 Hrs)

- o User interface overview (Lists, Libraries, Sites, Navigation)
- o Working with different site views
- o Search functionalities and filters
- o Introduction to SharePoint settings

Module 3: Creating and Managing Sites (05 Hrs)

- o Understanding different types of SharePoint sites (Team sites, Communication sites, etc.)
- o Creating new SharePoint sites (Modern & Classic)
- o Configuring site settings (navigation, branding, permissions)
- o Managing existing SharePoint sites

Module 4: Working with Lists and Libraries (07 Hrs)

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- ii. Creating and customizing lists and libraries
- c. Different types of list and library templates
- c. Adding and managing views (default, custom)
- c. Working with list/library items (creating, editing, deleting)
- c. Version control and content management

Module 5: Collaboration Features (07 Hrs)

- c. Document sharing and co-authoring
- c. Utilizing team calendars and tasks
- c. Working with workflows and approvals
- c. Using SharePoint news and announcements

Module 6: Security and Permissions (05 Hrs)

- b. Understanding user roles and permissions in SharePoint
- b. Setting permissions on sites, lists, and libraries
- b. Working with SharePoint groups and security best practices

Module 7: Search and Content Management (06 Hrs)

- b. Advanced search functionalities in SharePoint
- b. Metadata and content tagging for better organization
- b. Managing versions and content lifecycle
- b. Integrating SharePoint with other Office 365 apps

Module 8: Additional Resources and Best Practices (05 Hrs)

- c. Introduction to SharePoint development options (optional)
- c. Exploring Microsoft Learn for further training resources
- c. Sharing best practices for effective SharePoint usage
- c. Q&A and course wrap-up

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

3. COURSE: ADVANCED HARDWARE AND NETWORKING

Course Overview

This 100-hour course is designed to provide knowledge and practical skills necessary to understand computer hardware, network infrastructure, and their interaction. It prepares you for IT support roles. It emphasizing a 50/50 balance between theoretical knowledge and practical application.

Course Structure:

The course is divided into six modules, with hands-on labs, simulations, and practical exercises integrated throughout the program.

Module 1: Introduction to Computer Hardware (15 Hrs)

- o Components of a Computer System
- o Assembling and Disassembling a Computer
- o Operating Systems (OS) Fundamentals
- o Peripheral Devices: Troubleshooting Hardware Issues

Module 2: Advanced Hardware and Peripherals (15 Hrs)

- o Motherboard Components
- o Storage Technologies
- o Memory Management
- o Printers and Networking Peripherals
- o Troubleshooting Advanced Hardware Issues

Module 3: Networking Essentials (20 Hrs)

- o Network Fundamentals
- o Network Devices
- o Network Cabling and Standards
- o IP Addressing and Subnetting
- o Network Configuration and Management

Module 4: Local Area Networks (LANs) (20 Hrs)

- o LAN Design and Implementation
- o Network Operating Systems (NOS)
- o Network Security Fundamentals
- o Troubleshooting Network Connectivity Issues
- o Virtualization Technologies

Module 5: Wide Area Networks (WANs) and Network Services (20 Hrs)

- o WAN Technologies
- o Remote Access Solutions
- o Network Services (DNS, DHCP)

SCHEDULE OF REQUIREMENT
11BRD/4724/1/IT BM-II DATED 06 DEC 24

- o Network Monitoring and Troubleshooting Tools
- o Network Security Best Practices

Module 6: Simulations and Practice (10 Hrs)

- o Simulations and Practice Tests
- o Assessment
- o Regular quizzes and hands-on lab assessments throughout the course.
- o Practical exercises simulating real-world network troubleshooting scenarios.
- o Final exam to evaluate comprehensive understanding of course material.

Additional Considerations for all above mentioned IT courses:

- **Lab Environment:** A dedicated lab environment with various operating systems, network configurations, and vulnerable systems is essential for hands-on practice.
- **Tool Proficiency:** Ensure students gain proficiency in commonly used ethical hacking tools like Metasploit, Kali Linux, Burp Suite, and Wireshark.
- **Certification Alignment:** Align the curriculum with the latest CEH v12 exam objectives to maximize exam success.
- **Ethical Hacking Competitions:** Encourage students to participate in ethical hacking competitions to enhance practical skills and problem-solving abilities.

Delivery Methods

- Lectures and presentations
- Hands-on labs and exercises
- Group discussions and case studies
- Online resources and tools

Assessment

- Assignments and projects
- Practical exercises and code reviews
- Quizzes and exams
- Final project

Note: This curriculum provides a general outline and can be customized based on specific learning objectives, target audience, and available resources. It is essential to incorporate real-world examples, industry best practices, and emerging threats throughout the course.

Appendix 'B'
(Refers to Part II,
Para 1 (c) (iv) of the RFP)

QUALIFICATION AND EXPERIENCE OF INSTRUCTOR

Level of Course	Education Qualification	Experience on Teaching	Experience on Job	Desirable Qualification
Certified Ethical Hacker V12 CEH-v12	B Tech/M Tech (Comp Science/IT/Cyber Security)/MCA	(a) 5 Yrs in Training Industry (b) Associated and accredited trainer (c) Authorization from respective OEM (d) Should have conducted at least 10 batches of training independently	5 Years working Experience in relevant field/Project experience	EC-Council Certified Instructor Full time associated and accredited trainer
Certified Threat Intelligence Analyst (CTIA)				EC-Council Certified Instructor Full time associated and accredited trainer
Computer Hacking Forensic Investigator (CHFI)				EC-Council Certified Instructor Full time associated and accredited trainer
Certified Penetration Testing (CPENT)				EC-Council Certified Instructor Full time associated and accredited trainer
Certified Application Security Engineer (CASE)				EC-Council Certified Instructor Full time associated and accredited trainer
Advanced Web Designing/Full Stack Web Developer Using Python	B Tech/M Tech (Comp Science/IT)/MCA	(e) Good communication skills		Full time associated and accredited trainer
Advanced Hardware and Networking	B Tech/M Tech (Comp Science/IT)/MCA			CCNA Certified Instructor Full time associated and accredited trainer

FORMAT OF LESSON PLAN

Course Name :

Total Module :

Prepared by :

Module Index	Topic Index/ Module Description	Duration (Topic/Module covered in Hrs.)
1.	Introduction to Ethical Hacking	5 Hrs.
2.	Foot printing and Reconnaissance	5 Hrs.
3.	Scanning Networks	5 Hrs.
19.	Cloud Computing	5 Hrs.
20.	Cryptography	5 Hrs.
	and Continue	

Format of Block Training Programme:-

Days	Course Name	
	Session 1 (Morning)	Session 2 (Afternoon)
Day 1	Module 1, Module 2	Module 3
Day 2	Module 4, Module 5	Module 6, Module 7
Day 3	Module 8, Module 9	Module 10, Module 11
Day 4	Module 12,	Module 13, Module 14,
Day 5		
Day 6	And continue	

(Signature of Dean Academics/
 Director/CEO/ or Authorized
 Person)

STANDARDIZATION OF EXAMS

Depending upon the efforts required to solve a problem, the questions will have following difficulty levels.

Level-I : Questions which can be answered directly by selecting from given choices/clues.

Level II : Questions for which solution can be derived by applying simple formulae and - expressions.

Level-III : Questions for which Solutions can be derived by applying formulae / expressions to form an intermediate result and applying another formulae/expressions on them.

Module Tests are to be conducted at the end of each module and consisting of objective (MCQ, True/False, Fill-in-blanks and matching columns) descriptive types of questions are to be avoided whenever possible. Duration 60 minutes and maximum marks 100. For selection of questions, following criteria to be applied.

- (a) **Section I** : 20% questions of difficulty level -I.
(All Objective type)
- (b) **Section II** : 20% questions of difficulty level - II and 20% from level III.
(This section will consist of objective types)
- (c) **Section III** : 40% practical evaluation

At the end of the course, all the trainees are to be graded on a nine point scale based on their performance in the examinations/tests. The grading will be as per the following norms.

Grading index (in nine point scale)	Grade to be awarded
8.1-and above	Exceptional
7.0-8.0	Above Average
6.5-6.99	Average Plus
6.0-6.49	High Average
5.5-5.99	Average
Below 5.5	Below Average

Note: The above conditions are not applicable to EC Council course.

Appendix 'E'
(Refers to Part II,
Para 1 (i) (i) of the RFP)

ATTENDANCE SHEET

[illegible]

TECHNICAL BID PERFORMA
 (Use additional sheet where considered necessary)

Name of the Institute:

Description: Procurement of IT Training Courses

Sl No.	Applicable Clause of RFP		Clause	Acceptance (Yes/No)	Remarks (Append amplification Text, if any)
1.	Part I Para 15	Page No 6	Validity of Quotes/Bids (120 days from the last date of submission of the Bids)		
2.	Part I Para 16	Page No 6	The Bidders are required to submit Earnest Money Deposit (EMD) for an amount of Rs. 2,20,000/- along with bid.		
3.	Part I Para 18	Page No 6	Deduction of TDS		
4.	Part II Para 1	Page No. 7	Schedule of Requirement		
5.	Part II Para 4	Page No.11	Consignee (please specify)		
6.	Part-II Para 5	Page No. 11	Inspection Authority		
7.	Part III Para 9	Page No. 13	LD clause		
8.	Part IV Para 2	Page No.18	Performance Bank Guarantee @5%		
9.	Part IV Para 4	Page No.18	Tolerance Clause		
10.	Part IV Para 5	Page No.18	Payment Terms		

11.	Part IV Para 9	Page No 19	Fall Clause		
12.	Part-IV Para 10	Page No 20	Specification		
13.	Part IV Para 11	Page No 20	Franking Clause		
14.	Part V	Page No 22	Evaluation Criteria		
15.	Part V Para 3	Page No 22	Commercial/Price Bid Format		
16.	Part I Para 4 (e)	Page No 4	Whether certificates/documents submitted as per Annexure 'II'		
17.	All the other T&C's as mentioned in the RFP are also accepted				

Note: Bidders are advised to study the Tender/Bid Document carefully. Submission of the Bid shall be deemed to have been done after carefully studying and examination of all instructions, eligibility criterion, terms and requirement specification contained in the tender/Bid document with full understanding of its implications.

Annexure 'II'
(Refers to Part I Para 4 (e)
And Part II Para 2 of the RFP)

CERTIFICATES TO BE SUBMITTED ALONG WITH THE BID
(The prospective bidders will be Accepted/Rejected on the below mentioned certificates)

Sl. No.	Item Description/ Certificates/Documents	Documents/ Certificates to be submitted physically	Compliance by Institute (State whether submitted Yes / No)
1.	Earnest Money Deposit (EMD) (Refers to Part I Para 4 (a) & Part I Para 16 of the RFP)	EMD to be submitted	
2.	GST Reg. Certificate (Refers to Part I Para 4 (b) of the RFP)	GST registration certificate to be submitted	
3.	The copy of RFP duly stamped & signed on all pages (Refers to Part I Para 4 (c) of the RFP)	Stamped & Ink Signed copy of RFP (all Pages) to be submitted	
4.	Tender Acceptance Letter (Refers to Part I Para 4 (d) of the RFP)	Annexure- 'IV' of RFP to be submitted	
5.	Has the Institute been blacklisted by any of the offices of Central or State Govt. or any of its other customers? (Refers to Part I Para 5 (a) of the RFP)	Self-attested certificate to be submitted	
6.	Whether there is legal action being taken against institute for any cause in any legal jurisdiction in the last five years (Refers to Part I Para 5 (b) of the RFP)	Self-attested certificate to be submitted	
7.	Certificate of annual turnover (Refers to Part I Para 5 (c) of the RFP)	Audited annual accounts report of last three financial years	
8.	Institute should be an authorized training partner of EC Council (Refers to Part I Para 5 (d) of the RFP)	Authorization Certificate to be submitted	
9.	Trainer educational qualifications (Refers to Part I Para 5 (e) of the RFP)	Relevant certificate to be submitted	

10.	Accreditation/approval/Authorization certificate (Refers to Part I Para 5 (f) of the RFP)	Relevant certificate to be submitted	
11.	Proof of past training history (Refers to Part I Para 5 (g) of the RFP)	Relevant certificate to be submitted	
12.	Institute must have at least 10 years of experience in same field (Refers to Part I Para 5 (h) of the RFP)	Relevant certificate to be submitted	
13.	Whether Institute provide a valid verifiable course completion certificate. (Refers to Part I Para 5 (j) of the RFP)	Please state	
<p>Date: _____ Institute' Seal _____ Signature of Authorized Representative/Designation _____</p>			

Note: Institutes are requested to place all certificate/document serially and numbered

Institute's Name:

Annexure 'III'

(Refers to Part I Para 3

And Part V Para 3 of the RFP)

**FINANCIAL/COMMERCIAL BID PERFORMA FOR
IT TRAINING AT AIR FORCE STATION OJHAR**

Sl No.	Name of the courses including training materials	No. of course batch	Price per candidate	No of candidates in each course batch	Total (3X4X5)
1	2	3	4	5	6
(a)	Cyber Security Courses	5		20	
(b)	Full Stack Web Developer Using Python Backend	1		20	
(c)	Advanced Hardware and Networking	2		20	
(d)	Total Basic Price				
(e)	Any other item				
(f)	EC-Council Certification fee for Cyber Security Courses *	5		20	
(g)	Is GST extra? If yes, then mention the following:				
(i)	Total value on which GST is leviable:				
(ii)	Rate of GST:				
(iii)	Total value of GST leviable:				
(h)	Is Service Tax extra? If yes, then mention the following:				
(i)	Total value of Services on which Service Tax is leviable:				
(ii)	Rate of Service Tax leviable:				
(iii)	Total value of Service Tax leviable:				
(j)	Any other Taxes / Duties / Overheads / Other costs:				
(k)	Grand Total: (without adding row (f))				
	Grand Total amount in words (without adding row (f)):				
(l)	Grand Total: (with adding row (f)):				
	Grand Total amount in words (without adding row (f)):				

TENDER ACCEPTANCE LETTER
(To be submitted on Institutes' Letter Head)

To,
Air Officer Commanding,
11 BRD
Air Force Station
Ojhar, Nashik- 422221

Sub: Acceptance of Tender and Terms & Conditions of Tender.

Tender Reference No: **11BRD/4724/1/IT BM-II DATED 06 DEC 24**
Name of Tender: **INVITATION OF BIDS FOR PROCUREMENT OF IT TRAINING COURSES UNDER TWO BID SYSTEM**

Dear Sir,

1. I /We have downloaded/obtained the tender document(s) for the mentioned 'Tender' from the website/Mail:

as per your advertisement, given in the above mentioned website/Mail,

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

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

4. I /We hereby unconditionally accept the terms & conditions of above mentioned tender document(s)/corrigendum(s) in its totality/entirety.

5. In case any provisions of this tender are found violated, then your department/organization shall without prejudice to any other right or remedy be at liberty to reject this tender/bid including forfeiture of the earnest money deposit absolutely and necessary action be initiated as per terms & conditions of the tender document and extant rule of Govt. of India.

Yours Sincerely,

(Authorised Signatory with Official seal)