UNIVERSITY OF LAHORE (UOL)

Information Technology Services Division

REQUEST FOR PROPOSAL (RFP)

Comprehensive Cybersecurity Services | Fiscal Year 2026

DOCUMENT AT A GLANCE	
Issuing Organization	University of Lahore (UOL)
Document Title	RFP — Comprehensive Cybersecurity Services FY2026
RFP Reference No.	UOL/ITS/RFP/2026060812
Issue Date	June 2026
Proposal Submission Deadline	21-June-2026
SLA Commencement Date	01-July-2026
Contract Duration	One (1) Year from Date of Signing; one-year extension possible
Submission Portal / Email	tenders.uol.edu.pk
Contracting Authority	Director, Information Technology Services Division, UOL

1. Introduction and Background

The University of Lahore (UOL), one of Pakistan's leading private sector universities with a large and growing digital footprint across multiple campuses, hereby invites qualified and experienced vendors to submit proposals for the provision of Comprehensive Cybersecurity Services for Fiscal Year 2026.

UOL's Information Technology Services Division (ITSD) is responsible for securing the university's digital infrastructure, data assets, academic systems, financial platforms, and the personal information of thousands of students, faculty, and administrative staff. The evolving threat landscape — including ransomware, business email compromise, supply chain attacks, and insider threats — necessitates a robust, multi-layered security posture.

1.1 Objectives of this Engagement

- Strengthen UOL's cybersecurity posture against evolving and nation-state-grade threats.
- Enhance organizational resilience through proactive, detective, and reactive security capabilities.
- Ensure alignment with internationally recognized standards including ISO/IEC 27001, NIST CSF, and CIS Controls.
- Establish long-term partnerships with vendors who demonstrate innovation, operational maturity, and measurable value delivery.
- Build internal capability through knowledge transfer and security awareness programs.

1.2 Scope of Solicitation

This RFP is structured into five (5) independent Service Lots. Vendors may submit proposals for one or more lots. Each lot is evaluated independently; selection in one lot does not confer or preclude selection in another.

Lot	Title	Key Services
Lot 1	**Offensive Security Services**	Red Team, AD & Network Pen Testing, Source Code Review
Lot 2	**SOC & Threat Intelligence**	SOC L3, Threat Intel, Dark Web Monitoring, PIPT/EBP/DRP, SOAR, ISO 27001 Controls
Lot 3	**Digital Forensics & Incident Response**	End-to-End DFIR, RCA, Containment & Recovery, Post-Incident Reporting
Lot 4	**ISMS & Security Awareness**	Phishing Simulations, ISMS Implementation, User Awareness Programs
Lot 6	**ISO/IEC 27001 Certification Services**	Certification Audit, Certificate Issuance, Annual Audit, Recertification Audit
Lot 6	**Business Continuity & Disaster Recovery**	BCP Consultancy, DR Drills & Testing

2. Scope of Work

Lot 1 — Offensive Security Services

The vendor shall provide adversarial simulation and vulnerability identification services designed to test the effectiveness of UOL's defenses against realistic attack scenarios.

- **Red Team Exercises:** Full-scope adversarial simulation including physical, social engineering, and technical attack vectors, culminating in a detailed findings report with remediation roadmap.
- **Active Directory (AD) Penetration Testing:** In-depth assessment of AD configuration, privilege escalation paths, Kerberoasting, pass-the-hash, and lateral movement vectors.
- **Network Penetration Testing:** External and internal network assessments, firewall rule review, VLAN segmentation testing, and wireless security evaluation.
- **Source Code Review:** Static and dynamic analysis of internally developed applications for OWASP Top 10 and logic vulnerabilities.

Lot 2 — SOC & Threat Intelligence Services

The vendor shall augment or manage UOL's security monitoring and threat intelligence capabilities to ensure continuous visibility and rapid response.

- **SOC Level 3 Support:** Tier-3 analyst support for complex incident triage, threat hunting, malware reverse engineering, and escalated case management.
- **Threat Intelligence Services:** Curated, contextualized, and actionable intelligence feeds covering APTs, TTPs, and indicators of compromise relevant to the higher education and government sectors.
- **Dark Web Monitoring:** Continuous monitoring of dark web forums, paste sites, and criminal marketplaces for UOL credentials, data leakage, or reputational threats.
- **Protected Individual Impersonation Takedown (PIPT) / Executive Brand Protection (EBP) / Digital Risk Protection (DRP):** Detection and takedown of fraudulent social media profiles, fake domains, phishing pages, and brand impersonation targeting UOL executives and leadership.
- **SOAR Implementation & Optimization:** Deployment or optimization of Security Orchestration, Automation and Response playbooks to reduce mean-time-to-respond (MTTR).
- **SOC Controls Alignment (ISO 27001):** Gap assessment and remediation guidance to align SOC operations with Annex A controls of ISO/IEC 27001:2022.

Lot 3 — Digital Forensics & Incident Response (DFIR)

The vendor shall provide on-demand and retainer-based DFIR capability to respond to security incidents affecting UOL's systems, data, or operations.

- **End-to-End DFIR Services:** Full lifecycle incident response from initial detection through containment, eradication, recovery, and lessons-learned.
- **Complete Root Cause Analysis (RCA):** Forensic investigation to determine the full attack chain, patient zero, and contributing factors.
- **Incident Containment, Eradication & Recovery Support:** Active hands-on support to isolate affected systems, remove malicious artifacts, and restore operations.
- **Post-Incident Reporting & Recommendations:** Executive and technical reports suitable for regulatory disclosure, insurance purposes, and internal governance.

Lot 4 — ISMS & Security Awareness

The vendor shall support UOL's information security management system and foster a security-aware culture across the organization.

- **Phishing Simulation Campaigns:** Regularly scheduled and ad-hoc simulated phishing campaigns with measurement, reporting, and follow-up training.

- **ISMS Scope & Readiness Review**: Review of the ISMS boundaries, Statement of Applicability (SoA), and mandatory documentation to ensure organizational alignment with ISO/IEC 27001:2022 requirements.
- **Stage 1 (Readiness) Audit**: Preliminary assessment of the ISMS design and documentation to identify potential gaps and confirm UOL's preparedness for the formal certification audit.
- **User Security Awareness Programs:** Role-based, gamified, and multi-format awareness training tailored to academic, administrative, and technical staff.

Lot 5 — ISO/IEC 27001 Certification Services

The vendor shall provide independent, accredited certification and audit services to verify that UOL's Information Security Management System (ISMS) meets international standards.

- **Stage 2 (Certification) Audit:** Comprehensive technical and operational evaluation of the ISMS to verify the effective implementation of controls across the University IT Department, Data Center, and Cloud operations.
- **Accredited Certificate Issuance**: Provision of an internationally recognized ISO/IEC 27001:2022 certificate upon successful demonstration of compliance and closure of any identified non-conformities.
- **Annual Surveillance Audits**: Periodic on-site and remote audits conducted over the certification cycle to ensure the ongoing effectiveness and continuous improvement of the ISMS.
- **Recertification Audit**: Full-scope audit conducted at the end of the three-year cycle to renew the certification and assess the long-term maturity of UOL's security governance.

Lot 6 — Business Continuity & Disaster Recovery (BCP/DR)

The vendor shall ensure UOL's critical operations can withstand and recover from disruptive events.

- **Business Continuity Planning (BCP) Consultancy:** Development or review of BCP documentation, business impact analysis (BIA), and crisis management procedures aligned to ISO 22301.
- **Disaster Recovery (DR) Drills & Testing:** Tabletop exercises, simulation drills, and live DR tests with after-action reviews and improvement plans.

3. Eligibility & Minimum Qualification Requirements

All vendors must meet the following baseline eligibility criteria to be considered for evaluation. Non-compliance with any mandatory criterion will result in disqualification without further review.

3.1 General Eligibility

- The vendor must be a legally registered entity in Pakistan (or a foreign entity with a registered local partner or liaison office).
- The vendor must not be blacklisted, debarred, or under any regulatory sanction at the time of submission.
- The vendor must have been in active operation for a minimum of three (3) years in the cybersecurity domain.

3.2 Sector-Specific Reference Requirements

Vendors must demonstrate verifiable delivery of cybersecurity services in the following sectors, evidenced by reference letters on client letterhead or signed engagement summaries:

- **Service Sector (Retail):** At least one (1) client reference from a retail organization operating a minimum of fifteen (15) physical or digital outlets/branches, with an active engagement of at least six (6) months duration.
- **Financial Services Industry (FSI):** At least one (1) client reference from a nationally licensed commercial bank (as recognized by the State Bank of Pakistan or equivalent national regulator), with an active engagement of at least six (6) months duration.

3.3 Minimum Staffing Requirements

Vendors must demonstrate that the following resources are employed on a full-time, permanent payroll basis — not as contractors, freelancers, or secondments — and are available to be deployed on this engagement:

- A minimum of five (5) full-time employees per lot applied for, whose roles are directly relevant to the services proposed for that lot (e.g., penetration testers for Lot 1, SOC analysts for Lot 2, forensic examiners for Lot 3, etc.).

Proof of full-time employment must be furnished through:

- Copies of recent salary slips (last three consecutive months) for each named resource; AND
- Bank transaction records (salary credit entries) from the organizational payroll account for the same period, confirming actual salary disbursement to each named resource.

UOL reserves the right to conduct interviews with named resources and to verify employment records during due diligence. Any misrepresentation will result in immediate disqualification and possible blacklisting.

3.4 Certification Requirements

While not exhaustive, proposals will be evaluated more favourably where one or more of the following certifications are held by staff assigned to this engagement:

- CISSP, CISM, CRISC (governance/management)
- OSCP, GPEN, CEH, GREM (offensive security / Lot 1)
- GCFE, GCFA, EnCE (forensics / Lot 3)
- ISO 27001 Lead Auditor or Lead Implementer (ISMS / Lots 2, 4)
- CBCP, MBCI (business continuity / Lot 5)

4. Proposal Structure and Content Requirements

Proposals must be submitted in the order and format described below. Proposals that do not follow this structure may be evaluated at a disadvantage or disqualified.

4.1 Volume 1 — Technical Proposal

- **Section A: Executive Summary:** A concise (maximum 2 pages) overview of the vendor's proposed approach, key differentiators, and understanding of UOL's requirements.
- **Section B: Company Profile:** Legal registration details, organizational structure, years in operation, size of security practice, key executives, and relevant accreditations.
- **Section C: Technical Approach & Methodology:** Per lot applied for: detailed methodology, tools and platforms, frameworks referenced (MITRE ATT&CK, OWASP, NIST, ISO), quality assurance mechanisms, risk management approach, and escalation matrix.
- **Section D: Team Composition:** CVs of all personnel to be deployed on this engagement, including employment verification evidence (see Section 3.3). Clearly map each resource to the lot(s) they will support.
- **Section E: Relevant Experience & Case Studies:** Minimum two (2) case studies per lot applied for, each describing the client context, challenge, solution delivered, and measurable outcome. Reference letters must be appended.
- **Section F: Innovation & Value-Added Offerings:** Proprietary tools, automation capabilities, threat intelligence platforms, dashboards, or any additional services offered at no extra cost.

4.2 Volume 2 — Financial Proposal

Financial proposals must be submitted separately and sealed (if physical) or as a separate password-protected file. The password will be requested only from technically qualified vendors.

- Itemized pricing per service line within each lot applied for.
- Any bundled discounts for multi-lot engagement.
- Payment terms: UOL's standard terms are Net-30. Deviations must be explicitly noted.
- All prices in Pakistani Rupees (PKR) inclusive of applicable taxes. Indicate if GST is included or excluded.
- Vendors must use the standardized UOL Vendor Cost Submission Template (Excel format) provided as Annex A to this RFP.

4.3 Volume 3 — Administrative Documents

- Signed Proposal Transmittal Letter on company letterhead.
- Copy of SECP Registration / Trade License.
- Active NTN Certificate.
- Bank Statement or Audited Accounts for the last two (2) fiscal years (demonstrating financial viability).
- Signed statement confirming no conflict of interest with UOL.
- Signed acknowledgement of UOL's IP Ownership clause (Section 8.2).

5. Evaluation Methodology

UOL will employ a two-envelope, quality-and-cost-based selection (QCBS) methodology consistent with international procurement best practice (aligned to World Bank Procurement Regulations, 2020 Edition). Technical and financial proposals are evaluated independently by separate committees.

5.1 Evaluation Scoring Formula

The final composite score for each technically qualified vendor is calculated using the following weighted formula:

```
Final Score = (Technical Score × 0.65) + (Financial Score × 0.35)
```

Where:

- Technical Score = weighted sum of sub-criteria scores (see table below), normalized to 100.
- Financial Score = (Lowest Evaluated Price / Vendor's Price) × 100.

Note: Only vendors achieving a minimum Technical Score of 70/100 will have their financial proposals opened. This threshold ensures that cost competition occurs only among technically capable vendors, consistent with World Bank QCBS methodology.

5.2 Technical Evaluation Criteria and Weights

The three (3) technical sub-criteria are weighted as follows. Each sub-criterion is scored by the Evaluation Committee on a scale of 0–100, then multiplied by its weight to produce a weighted score.

Criterion	Weight	Max Score (100)	Description
Technical Expertise & Certifications	30%	30	Qualifications, certifications (CISSP, CISM, ISO 27001 Lead Auditor, OSCP, etc.), tooling, methodology depth, and quality of proposed approach.
Relevant Experience & Track Record	35%	35	Demonstrated delivery of similar services for FSI and retail-sector clients of comparable scale; case studies; client references; team CVs.
Cost-Effectiveness & Pricing	35%	35	Competitive, transparent cost structure; value for money; bundled discounts; payment terms and total cost of ownership.
TOTAL	**100%**	**100**	

5.3 Scoring Guidance for Evaluators

Scores within each criterion band shall be awarded as follows:

Score Band	Rating	Guidance
90–100	**Exceptional**	Exceeds requirements; demonstrates market-leading capability with verifiable evidence.

75–89	**Strong**	Fully meets requirements with substantial verifiable evidence.
60–74	**Adequate**	Meets most requirements; minor gaps noted.
40–59	**Marginal**	Partially meets requirements; significant gaps or unsubstantiated claims.
0–39	**Inadequate**	Does not meet requirements or fails to provide evidence.

5.4 Disqualification Criteria

Proposals will be automatically disqualified for any of the following:

- Failure to meet any mandatory eligibility criterion (Section 3).
- Submission after the stated deadline.
- Material misrepresentation in any section of the proposal.
- Failure to submit employment verification evidence for the minimum five (5) full-time staff per lot.
- Conflict of interest not disclosed.

6. Contract Terms & Conditions

6.1 Contract Duration

The initial contract term shall be one (1) year commencing from the date of contract signing by both parties. UOL targets a SLA commencement date of 01-July-2026, subject to the timely completion of procurement and NDA/contract execution.

6.2 Contract Extension

UOL reserves the right to extend the contract for one (1) additional year upon expiry of the initial term, subject to the following conditions:

- The vendor has demonstrated exemplary performance across all contractual KPIs and SLAs during the initial term, as assessed through UOL's formal Vendor Performance Review process.
- An automatic price adjustment of seven percent (7%) above the original contracted rates will apply in the event of extension. No further negotiation on this delta is permitted.
- Extension shall be formally communicated in writing no later than sixty (60) days prior to contract expiry.

6.3 Service Level Agreements (SLAs)

Vendors must propose SLAs for each service line within their submitted lots. Minimum expected SLA parameters include:

Service Area	SLA Metric	Minimum Threshold
SOC Monitoring (Lot 2)	Alert Triage SLA (P1)	15 minutes from detection
SOC Monitoring (Lot 2)	Incident Escalation (P1)	30 minutes from triage
DFIR Retainer (Lot 3)	On-site/Remote Response Mobilization	4 hours from declaration
DFIR Retainer (Lot 3)	Preliminary Report Delivery	48 hours post-containment
Pen Testing (Lot 1)	Draft Report Delivery	5 business days post-testing
BCP/DR (Lot 5)	DR Test Completion per Cycle	Annual, per agreed schedule

6.4 Performance Monitoring

- Monthly service review meetings between UOL ITSD and the vendor.
- Quarterly formal performance scorecards issued by UOL.
- Vendor must maintain and submit monthly activity reports for all contracted services.
- Failure to meet SLAs for two (2) consecutive months may result in penalty deductions or contract termination at UOL's discretion.

6.5 Termination for Convenience

UOL reserves the right to terminate any contract with thirty (30) days written notice. In such cases, the vendor shall be compensated for work satisfactorily completed up to the notice date.

7. Legal, Compliance & Intellectual Property

7.1 Confidentiality

This RFP and all information furnished in connection with it are strictly confidential. Vendors must not disclose any content of this RFP, or any organizational data, systems, processes, or information encountered during the engagement, to any third party without prior written consent from UOL. Unauthorized disclosure will be treated as a material breach.

7.2 Intellectual Property (IP) Ownership

All intellectual property, tools, scripts, frameworks, reports, documentation, methodologies, code, playbooks, or any other deliverable created, developed, or customized by the vendor specifically within the scope of this engagement, and at the premises, systems, or cost of the University of Lahore, shall become the sole and exclusive property of the University of Lahore (UOL) upon delivery and acceptance.

Vendors shall ensure that:

- All deliverables are free of third-party IP encumbrances or open-source licensing restrictions that would limit UOL's ownership or use.
- Any pre-existing vendor IP (background IP) incorporated into deliverables is clearly identified and licensed to UOL on a perpetual, royalty-free basis for use within the scope of this engagement.
- A signed IP Assignment Agreement will be executed as part of the contract.

7.3 Non-Disclosure Agreement (NDA)

Vendors shortlisted for award will be required to execute a Non-Disclosure Agreement (NDA) with UOL as a condition precedent to contract finalization. The NDA will cover:

- All organizational, technical, financial, and student data encountered during the engagement.
- All findings, vulnerabilities, and intelligence gathered during service delivery.
- Personnel information and system architecture details.

Execution of the NDA is mandatory. Vendors who decline will be disqualified from the award process.

7.4 Data Protection & Compliance

- Vendors must comply with all applicable data protection regulations and UOL's internal data handling policies.
- No data, findings, or vulnerability information may be retained by the vendor beyond the contractual retention period agreed in writing.
- Vendors must implement appropriate technical and organizational controls to protect any UOL data in their possession.

7.5 Conflict of Interest

Vendors must disclose any actual or potential conflict of interest at the time of proposal submission. Failure to disclose a material conflict of interest is grounds for disqualification and potential blacklisting.

7.6 Force Majeure

Neither party shall be liable for failure to perform contractual obligations caused by circumstances beyond their reasonable control, provided that the affected party promptly notifies the other party in writing and takes all reasonable steps to mitigate the impact.

8. Submission Requirements & Procurement Timeline

8.1 Submission Format

- Proposals must be submitted in electronic format as PDF files (for Volumes 1 and 3) and Excel format (for Volume 2 / Financial Proposal).
- File naming convention: [VendorName]_[LotNumber]_[Volume]_RFP2026SEC001. Example: ABCSecurity_Lot1_TechnicalProposal_RFP2026SEC001.pdf
- All files must be submitted to [Insert Email / Portal URL] by [Insert Deadline].
- The Financial Proposal file must be password-protected. The password will be communicated separately upon request by UOL.
- Late submissions will not be considered under any circumstances.

8.2 Procurement Timeline

#	Milestone	Target Date	Responsible Party
1	RFP Issuance	June 2026	UOL ITSD
2	Deadline for Written Clarifications	15-June-2026	Vendors
3	UOL Responses to Clarifications	18-June-2026	UOL ITSD
4	Proposal Submission Deadline	21-June-2026	Vendors
5	Technical Evaluation	23-June-2026	Evaluation Committee
6	Financial Evaluation	23-June-2026	Evaluation Committee
7	Vendor Presentations / Demos (if req.)	24-June-2026	Shortlisted Vendors
8	Award Notification	26-June-2026	UOL ITSD
9	NDA & Contract Signing	29-June-2026	Selected Vendor(s)
10	**SLA Commencement**	01-July-2026	All Parties

8.3 Contact Information

For all procurement-related enquiries, please contact:

Contact Person	Muhammad Zeeshan Khan Sherwani
Designation	Assistant Director Data Center & Applications
Organization	University of Lahore (UOL)
Email	projects@its.uol.edu.pk
Phone	042 35322501-10 Ext: 5027
Office Address	The University of Lahore, Main Campus, 1-Km Defence Roadd, near Bhuptian Chowk, Raiwind Road Lahore

8.4 General Disclaimer

- UOL reserves the right to accept or reject any or all proposals, to waive minor informalities, and to award contracts in the best interest of the university.
- UOL is not obligated to disclose reasons for rejection.
- This RFP does not constitute a commitment to procure any services.
- UOL will not reimburse vendors for any costs incurred in the preparation and submission of proposals.

— END OF REQUEST FOR PROPOSAL —

UOL/ITSD/RFP/2026/SEC-001 | Confidential | University of Lahore