DIGITAL UNIVERSITY KERALA
Curating a responsible digital world

Kerala University of Digital Sciences,
Innovation and Technology (Digital University)
Technocity Campus, Mangalapuram, Thonnakkal PO,
Thiruvananthapuram, Kerala - 695 317

Tel : +91- 471- 2788000
Email : info@duk.ac.in
www.duk.ac.in

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 1

No. KUDSIT/587/AD AIII/2023 Dated: 27.10.2026

NOTIFICATION

Kerala University of Digital Sciences, Innovation and Technology invites applications from qualified Indian Citizens for appointment to the following post (on a contract basis) for KSAAC project of the University. Candidates shall apply online through the Recruitment Portal. The guidelines for the submission of applications are available in the recruitment portal.

DETAILS OF POST, QUALIFICATION, EXPERIENCE ETC. REQUIRE.

I. Lead Auditor

Job code	LA/102026/587
Name of Post	Lead Auditor
No. of Vacancies	One
Remuneration	Rs.80,000 - 85,000(consolidated)
Age	Should not exceed 40 years as of the last date for submission of application
Essential Educational Qualification	B.E./B.Tech./M.E./M.Tech./MCA/M.Sc. in Computer Science, Information Technology, Cybersecurity or a related discipline from a recognised University/Educational Institution.
Essential Experience	• A minimum of 12 years of relevant professional experience in cybersecurity, information security auditing, security assessments or related fields. • Demonstrated experience in planning, leading, conducting and reviewing cybersecurity audits and security assessments. • Experience in one or more of the following areas: Web Application Security Auditing, Mobile Application Security Auditing, IT Infrastructure Security Auditing, Vulnerability Assessment and Penetration Testing (VAPT), Secure Code Review and information security compliance assessments.

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 2

	• Experience in audit methodology development, risk assessment, vulnerability validation, evidence review, audit reporting and recommending corrective actions. • Experience in leading technical teams, reviewing audit deliverables, ensuring quality standards and coordinating with clients and stakeholders.
Desirable skillset	• Relevant internationally recognised certifications such as ISO/IEC 27001 Lead Auditor, CISA, CISSP, CISM, CPENT, CEH or equivalent. Multiple relevant certifications will be an advantage. • Demonstrated experience in leading end-to-end cybersecurity audit engagements, including scope definition, audit planning, resource allocation, execution, quality review and final report submission. • Good knowledge of applicable CERT-In directions and guidelines, recognised cybersecurity frameworks, ISO/IEC 27001, NIST frameworks and relevant security auditing standards. • Experience in developing and implementing standard operating procedures, audit checklists, methodologies, quality assurance processes and report templates. • Ability to evaluate security findings, assess risks, determine severity and business impact, and recommend practical remediation measures. • Experience in handling cybersecurity audit assignments for Government departments, PSUs, universities, autonomous institutions or private-sector organisations will be an advantage. • Experience in supervising and mentoring security analysts, auditors and technical specialists. • Excellent technical report-writing, presentation, communication, team leadership and client-management skills. • Experience in supporting proposals, Statements of Work (SoW), project planning, audit estimates and client consultations will be an advantage.
	• Lead and manage cybersecurity auditing engagements undertaken by KSAAC in accordance with applicable requirements, approved methodologies and organisational quality assurance procedures.

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 3

Job Description	• Plan, coordinate and supervise cybersecurity audits and assessments, including Web Application Security Auditing, Mobile Application Security Auditing, IT Infrastructure Security Auditing, VAPT and Secure Code Review. • Define audit scope, objectives, methodology, timelines, resource requirements and deliverables in consultation with the competent authority and relevant stakeholders. • Allocate assignments to audit team members, monitor progress, provide technical guidance and ensure timely completion of audit activities. • Review and validate audit findings, supporting evidence, risk ratings, technical observations and remediation recommendations. • Ensure that audit reports are accurate, evidence-based, technically sound and compliant with approved reporting and quality standards. • Oversee the preparation and submission of draft and final audit reports, executive summaries, risk registers and remediation recommendations. • Maintain regular liaison and professional coordination with CERT-In to obtain and disseminate relevant updates concerning applicable directions, guidelines, advisories, empanelment-related requirements and cybersecurity auditing practices. • Monitor relevant CERT-In notifications and regulatory developments, assess their implications for KSAAC's auditing activities and recommend necessary updates to audit methodologies, procedures, checklists and internal practices. • Coordinate with the concerned authorities and ensure timely communication and follow-up on matters relating to applicable CERT-In requirements and organisational responsibilities. • Develop and maintain audit methodologies, standard operating procedures, checklists, templates, quality assurance processes and internal technical documentation. • Mentor and develop the technical capabilities of security auditors and analysts through technical reviews, knowledge-sharing sessions and professional development activities.

	• Coordinate with client organisations to clarify technical observations, discuss audit findings and facilitate the closure of audit assignments. • Monitor audit progress, identify delivery risks, resolve technical issues and escalate matters requiring management intervention. • Support the preparation of technical proposals, Statements of Work, project estimates and responses to requests for proposals related to cybersecurity auditing and consultancy. • Contribute to the continuous improvement and expansion of KSAAC's cybersecurity auditing and assurance services. • Perform any other duties related to cybersecurity auditing, quality assurance, technical leadership and institutional coordination as assigned by the competent authority.
Nature of Appointment	On contract basis for One Year. However, the term may be extended further based on the performance and project requirements.

II. Cybersecurity Solutions Architect

Job code	CSA/102026/587
Name of Post	Cybersecurity Solutions Architect
No. of Vacancies	One
Remuneration	Rs.70,000 - 75,000(consolidated)
Age	Should not exceed 40 years as of the last date for submission of application
Essential Educational Qualification	B.E./B.Tech./M.E./M.Tech./MCA/M.Sc. in Computer Science, Information Technology, Cybersecurity or a related discipline from a recognised University/Educational Institution.
	• A minimum of 10 years of relevant professional experience in cybersecurity, networking, system administration, cybersecurity consulting, solution design or related fields. • Experience in designing cybersecurity solutions, conducting security assessments, and preparing technical proposals and project reports.

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 4

Essential Experience	• Experience in at least some of the following areas: Vulnerability Assessment and Penetration Testing (VAPT), application security, network and infrastructure security, cloud security, security governance, risk and compliance. • Experience in client engagement, requirement analysis, solution presentation and coordination with technical teams.
Desirable skillset	• Relevant internationally recognised certifications such as ISO/IEC 27001 Lead Auditor, CISA, CISSP, CISM, CPENT, CEH or equivalent. Multiple relevant certifications will be an advantage. • Good knowledge of cybersecurity frameworks and standards, including ISO/IEC 27001, NIST Cybersecurity Framework and applicable CERT-In directions and guidelines. • Ability to design and recommend security architectures, cybersecurity solutions, technical controls and implementation roadmaps based on organisational requirements. • Experience in preparing technical proposals, techno-commercial bids, project estimates, Statements of Work (SoW), consultancy reports and project documentation. • Experience in business development, client relationship management, institutional partnerships and identifying cybersecurity consulting and audit opportunities. • Experience working with Government departments, Public Sector Undertakings (PSUs), universities, autonomous institutions or private-sector organisations will be an advantage. • Excellent communication, presentation, analytical, coordination and report-writing skills.
	• Design and recommend cybersecurity solutions and secure architectures for applications, networks, IT infrastructure, cloud environments and enterprise systems. • Analyse client requirements and develop appropriate cybersecurity solutions, technical approaches and implementation roadmaps. • Support the planning and delivery of cybersecurity

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 5

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 6

Job Description	services, including VAPT, application security audits, infrastructure security audits, secure code review, digital forensics, information security governance, risk assessment and compliance services. • Prepare technical proposals, techno-commercial bids, project estimates, Statements of Work (SoW), service descriptions and consultancy reports. • Identify new business opportunities and support the expansion of cybersecurity audit, consultancy, training and compliance services offered by KSAAC. • Establish and maintain professional relationships with Government departments, PSUs, universities, industries and other prospective clients and institutional partners. • Support business development activities for KSAAC and DUK by identifying consultancy projects, collaborative opportunities, industry partnerships and potential revenue-generating activities. • Coordinate with internal technical teams and subject-matter experts to develop proposals, present solutions and ensure that proposed services are technically feasible and aligned with client requirements. • Participate in client meetings, technical presentations, project discussions, negotiations and proposal follow-ups. • Monitor emerging cybersecurity technologies, industry trends, regulatory developments and market requirements to identify opportunities for new services. • Assist in developing service catalogues, standard methodologies, pricing models and delivery frameworks for cybersecurity consulting and audit services. • Perform any other duties related to cybersecurity consultancy, solution architecture, institutional collaboration and business development as assigned by the competent authority.
Nature of Appointment	On contract basis for One Year. However, the term may be extended further based on the performance and project requirements.

III. Junior Forensics Analyst

Job code	JFA/102026/587
Name of Post	Junior Forensics Analyst

No. of Vacancies	One
Remuneration	Rs.20,000 - 25,000(consolidated)
Age	Should not exceed 30 years as of the last date for submission of application
Essential Educational Qualification	B.E./B.Tech./BCA/MCA/M.Sc. in Computer Science, Information Technology, Cybersecurity, Digital Forensics or a related discipline from a recognised University/Educational Institution.
Essential Experience	• Experience is not mandatory. • Fresh graduates may apply. Candidates with up to one year of relevant experience in digital forensics, cybersecurity, incident response or related fields will also be considered. • Basic knowledge of computer systems, operating systems, file systems, storage devices and networking. • Basic understanding of digital evidence identification, preservation, acquisition and forensic examination. • Familiarity with Windows and Linux operating systems and command-line tools. • Ability to document technical procedures, maintain records and prepare clear technical reports.
Desirable skillset	• Relevant certifications or training in digital forensics, incident response, cybersecurity or computer investigations. • Familiarity with digital forensic tools such as Autopsy, The Sleuth Kit, FTK Imager, Magnet AXIOM or equivalent tools. • Basic knowledge of disk imaging, file-system analysis, deleted-file recovery, metadata examination, hash verification and timeline analysis. • Awareness of forensic chain of custody, evidence integrity, evidence handling procedures and the importance of maintaining forensic working copies. • Basic understanding of mobile device forensics, browser artefact analysis, email forensics, log analysis and malware-related investigations. • Familiarity with scripting or programming languages such as Python, Bash or PowerShell will be an advantage. • Good analytical, problem-solving, documentation and

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 7

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 8

	communication skills. • Willingness to learn new forensic tools, techniques and investigative methodologies.
Job Description	• Assist senior forensic professionals in digital forensic investigations involving computers, storage media, mobile devices, logs and other digital sources, as assigned. • Assist in the identification, preservation, acquisition and examination of digital evidence in accordance with approved procedures and applicable authorisations. • Perform forensic disk imaging, hash verification, file-system analysis, metadata examination, deleted-file recovery and other basic forensic examination tasks under supervision. • Assist in analysing system artefacts, browser history, application artefacts, event logs and other relevant digital traces. • Support the collection, organisation, preservation and documentation of digital evidence while maintaining appropriate chain-of-custody records. • Use approved forensic tools and follow established procedures to maintain evidence integrity and reproducibility of examination results. • Assist in preparing forensic examination notes, evidence inventories, technical observations and draft forensic reports. • Maintain proper documentation of tools used, examination steps, findings, limitations and supporting evidence. • Support senior team members in incident response, cybercrime investigations, malware-related examinations and other digital forensic assignments, where required. • Assist in maintaining forensic laboratory equipment, software, evidence storage systems and case documentation. • Keep abreast of developments in digital forensics, forensic tools, investigation techniques and relevant technical guidelines. • Participate in internal training, knowledge-sharing sessions and technical skill-development activities • Perform any other duties related to digital forensics,

	cybersecurity investigations and technical documentation as assigned by the competent authority
Nature of Appointment	On contract basis for One Year. However, the term may be extended further based on the performance and project requirements.

Age relaxation for submission of application

5 years for candidates belonging to SC/ ST and 3 years for OBC candidates.

Mode of Selection

The selection will be based on a test and/or Interview

Venue of Test/Interview

The test /Interview will be conducted in Thiruvananthapuram district only.

Job Location

For all posts will be at Thiruvananthapuram

General Instructions

1. Scanned copy of the documents to prove age, qualifications, experience, etc. should be uploaded along with online application and originals to be produced as and when called for. Applications without attaching the above documents shall be summarily rejected. No further chance will be given for submitting the same.
2. Incomplete applications or applications without filling the relevant fields will be summarily rejected.
3. Candidates should ensure that the particulars furnished by him/her are correct in all respects. Anything not specifically claimed in the application against the appropriate field will not be considered at a later stage. No deviation whatsoever from the filled in data will be entertained. In case it is detected at any stage of the recruitment that a candidate does not fulfill the eligibility norms and /or that he/she furnished any incorrect/false information or has suppressed any material fact, his/her candidature will stand cancelled. If suppression of material facts or furnishing of any incorrect/false information is detected even after appointment, his/her service is liable to be terminated.
4. Applications submitted without fulfilling the eligibility and other norms mentioned in this Notification as well as the instructions published in the Recruitment Portal of the University will be summarily rejected.
5. In case any discrepancy / ambiguity in the process of selection, the decision of the University shall be final and binding.
6. Consequent up on adoption of self- certification provisions, the University shall process the applications entirely on the basis of the information/documents provided with the application. The selection / appointment will be provisional and subject to physical verification of the documents.
7. Canvassing in any form will entail the cancellation of candidature.

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 9

How to Apply:

1. Applications shall be submitted online latest on **15.11.2026**. The application form is available at https://www.duk.ac.in/careers.
2. The applications received after the last date fixed or the incomplete applications or the applications without filling the relevant field will be summarily rejected.
3. No interim queries after the submission of the application will be entertained. The candidates will be intimated the schedule of the Test/ Interview through their registered email only.
4. The candidates are advised to check their registered e-mails regularly after the last date fixed for the submission of the application.
5. The University has the right to cancel the advertisement or entire selection process at any stage without assigning reason thereof and the decision of the University shall be final.

Registrar

* This is a computer system (Digital File) generated letter. Hence there is no need for a physical signature.

Draft #33 of File KUDSIT/587/AD AIII/2025 Approved by Registrar on 31-Oct-2026 02:27 PM - Page 10