Designation	Center Head (CH)
Responsibilities	Lead the operational aspects of the Centre of Excellence in Cybersecurity, Govt of Karnataka (CySecK CoE), supported by the Dept of IT, BT and S&T, GoK and the Karnataka Innovation and Technology Society (KITS). The objectives of the CoE are organized into 4 pillars: *Skill building* *Promotion of industry and start-ups* *Supporting state government departments with cyber risk management* *Research and innovation* The responsibilities of the CH include the following: • Set up and streamline the processes for the operationalization of the CoE initiatives, and its day-to-day management • Ensure that the CoE achieves its goals • Strategize and define immediate, mid-term and long-term action plans, as well as implement and maintain programme initiatives consistent with the CoE objectives • Monitor the global cybersecurity landscape for relevant developments and breaking news • Work with the Convenor to assemble a team to systematically execute all CoE activities • Track the status of deliverables, provide updates to various levels of stakeholders and take corrective actions whenever needed • Interact with IISc faculty and research students, the cybersecurity industry ecosystem, government departments working in the cybersecurity space to ensure that the CoE becomes the "go to" place for cybersecurity matters
Employment type	Full-time, fixed-term contract for three years, initially with six-month probation. Based on requirements and performance, the contract can be extended by mutual consent.
Remuneration	Commensurate to with experience and skill set, competitive with the industry
Location	Bengaluru
Education	1. ME/MTech or above in Electrical, Electronics, or Computer Science or allied disciplines or

	2. BE/BTech in Electrical, Electronics, or Computer Science or allied disciplines and/or Management degree
Experience level	Overall experience of 5+ years with at least 2 years in Project / Program Management and relevant R&D experience. These could be relaxed in the case of candidates with an exceptional track record.
Technical skills	• Experience in cyber security policy and practice, knowledge of security vulnerabilities, security measures threat modeling approaches, and tools. • Understanding of network attacks, DDoS, encryption, authentication, logging and log analysis, security rules and policies, and knowledge of related protocols (e.g., TCP/IP, TLS, routing protocols). • Understanding of database security, data encryption, data desensitization, data backup, and managing identity and access such as role-based access control. • Exposure to cyber security audit mechanisms of and exposure to standards-based security assessment (ISO 27001), cyber security frameworks such as that of NIST
Management Skills	• Knowledge of programme management principles, and processes, strong interpersonal skills, people management and mentoring skills, ability to work in small teams and manage projects independently • Excellent verbal and written communication in English and Kannada • Strong moral compass and that will uphold organizational values of public service, ethics, and integrity • Ability to interact with and manage senior-level stakeholders in government, academia, and industry
Selection Process	After the closing date, the applications will be screened, and shortlisted candidates will be called for personal interviews. IISc and FSID reserve the right to interview only a subset of the candidates.
How to Apply	Please send your CV with a cover letter and any other relevant supporting documents as a single PDF document to kuri@iisc.ac.in, with the subject line "CySecK CoE" For any queries, please email kuri@iisc.ac.in, with the same subject line.
Closing date	**23 September 2024**