



המרכז לחקר הסייבר, משפט ומדיניות
The Center for Cyber Law & Policy
المركز لبحث السايبر، السياسة والقانون
אוניברסיטת חיפה UNIVERSITY OF HAIFA



INCD
Israel National
Cyber Directorate

THE CENTER FOR CYBER, LAW & POLICY and its BIOMETRICS SUBCENTER

CALL FOR PROPOSALS 2026

The Center for Cyber, Law and Policy (CCLP), in collaboration with the Israeli National Cyber Directorate, invites scholars, researchers from academia and industry (including faculty, post-doctoral researchers, and graduate students) with expertise in cyber/biometrics law, policy or technology, to apply for research grants in the tracks described below. **Applications must be submitted no later than: Sunday, 15 April 2026.**

Research proposals should follow the instructions and relate to the themes as detailed below. Be sure to specify the track for consideration and matching funds (if applicable).

1. *Research Track*

Eligibility: Faculty members of any accredited academic institution in Israel and prominent academics or professional experts, from Israel or abroad, working in collaboration with a faculty member as Co-PIs on a joint proposal.

Funding: The CCLP offers research grants up to NIS 100,000 (in addition to the researcher's matching budget) for one calendar year. There will be a possibility to request one additional year of funding towards the end of the initial grant period. Proposals addressing aspects prominently related to biometrics (on its own or in relation to cyber) may receive up to 150,000 NIS.

To further encourage researchers to approach their research in an interdisciplinary manner, we allow Research Track proposals to collaborate as a **Research Group** of at least three researchers. The Research Track proposals shall be submitted together with an additional document (up to one page) emphasizing the expected synergy between the projects.

2. *Fellows Track*

Eligibility: Graduate students of any accredited academic institution in Israel interested in pursuing a research project towards an academic publication.

Funding: up to NIS 50,000 (in addition to the hosting researcher's matching budget) for one calendar year. There will be a possibility to request one additional year of funding towards the end of the initial grant period.

3. *Visiting Researchers Track*

Eligibility: Faculty, fellows, and doctoral students of any accredited foreign academic institution interested in visiting CCLP for two weeks or more.

Funding: CCLP will cover travel and accommodation expenses throughout the visit.



RESEARCH THEMES

CCLP will support selected proposals related to cyber, biometrics, quantum or the intersection thereof. Proposals may approach these topics and themes from legal, ethical, or technological perspectives:

1. Malicious Artificial Intelligence and AI-Driven Cyber Warfare

- Use of artificial intelligence as an offensive cyber capability, including autonomous or semi-autonomous cyber operations.
- AI-enabled malware, adaptive attack techniques, and automated exploitation of vulnerabilities, emphasis on Digital Identity and/or Identity Management Systems.
- Adversarial machine learning and attacks against AI-based cyber defense systems.
- Legal, ethical, and strategic implications of AI-driven cyber warfare, including attribution, deterrence, escalation, accountability and disruption.
- Malicious use of AI for cyber attacks in conflicts and information warfare by state and non-state actors.

2. Artificial Intelligence in the Use and Governance of Cyber Tools

- Use of AI in decision-making cybersecurity processes, including monitoring, control, enforcement, and governance of digital systems and infrastructures, such as Digital Identity and/or Identity Management Systems.
- Human versus machine decision-making in cybersecurity operations, including human-in-the-loop, human-on-the-loop, and fully automated use of cyber tools.
- Explain-ability and interoperability, accountability, and due process in AI-supported cyber decisions, particularly where automated systems affect rights.
- Risks arising from reliance on AI-driven cyber tools, including bias, error propagation, loss of human oversight, and unintended systemic effects.
- Legal and policy frameworks governing AI-enabled use of cyber tools, including standards for oversight, responsibility, and accountability.
- Economics of AI based cybersecurity.
- Deception and evasion by AI tools against AI based cybersecurity

3. Quantum and Post-Quantum Cybersecurity

- Applied research in quantum-secure communications, including Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC).
- Hybrid architectures combining quantum and post-quantum cryptographic mechanisms for resilience and cryptographic agility.
- Practical deployment challenges of post-quantum security in telecommunications, cloud infrastructures, Digital Identity and/or Identity Management Systems and critical systems.



המרכז לחקר הסייבר, משפט ומדיניות
The Center for Cyber Law & Policy
المركز لبحث السايبر، السياسة والقانون
אוניברסיטת חיפה UNIVERSITY OF HAIFA



INCD
Israel National
Cyber Directorate

- Validation, testing, and performance metrics for post-quantum security technologies.

Quantum Technologies: Policy, Legal and Economic Implications at the Intersection of Cybersecurity, Communications Protection, and the Transition to Quantum-Safe Infrastructures

APPLICATION SUBMISSION

All applications must be completed in English and submitted electronically, clearly stating the submission track.

Applications should include:

1. A Research Proposal: up to a three-page description of the proposed research and its relevance to the current call (plus one page for references). Additional supporting material may be submitted and read at the reviewers' discretion.

The research proposal should include:

- a. A clear presentation of the research questions, their relevance to a specific theme, state of the art, the proposed solutions, methodologies, or technical approaches the research intends to set forth, and their novelty.
 - b. The qualification of the research team to perform the proposed research.
 - c. A research plan and timetable demonstrating the feasibility of conducting the proposed research within the time and funding limitations.
 - d. A Research Budget: please see Annex for guidelines. Where applicable, indicate whether other sources provide additional support. More specifically, if you have non-Israeli-government funds which may be, or are, allocated to support the proposed research or components thereof, please be sure to state the sum and source, as this increases the chances of funding.
2. Curriculum Vitae of PIs, including a list of selected publications (up to 5 pages).
 3. List of 3-5 international experts in the field of research (cannot be: affiliated with the institutions of the researcher(s) submitting the proposal, supervisors/supervisees of the researcher(s), co-authored in the last 3 years, or personal relationship).

REVIEW PROCESS

All proposals will be peer-reviewed. Selection for funding will be determined by CCLP's Scientific Committee on the basis of academic excellence and the availability of resources. All funding decisions are subject to approval by the CCLP and the Biometrics' sub-center Steering Committee. CCLP reserves complete discretion regarding awarding grants, including the option of not awarding any grant under this CfP.



המרכז לחקר הסייבר, משפט ומדיניות
The Center for Cyber Law & Policy
المركز لبحث السايبر، السياسة والقانون
אוניברסיטת חיפה UNIVERSITY OF HAIFA



INCD
Israel National
Cyber Directorate

GENERAL TERMS AND CONDITIONS

Grant recipients will be expected to:

1. Lead their research agenda, as well as collaborate with the CCLP faculty and fellows, and contribute to the building of its academic community and reputation.
2. Participate in and present their work at a CCLP event.
3. Submit a final research report describing the outcome of the research and/or intermediate report, upon request.
4. Submit a paper for publication resulting from the research. Each publication supported by the grant will include an acknowledgment.

SUBMISSION

Completed applications must be sent to cyber@univ.haifa.ac.il and received by **15 April 2026**.
For any additional questions, please do not hesitate to contact us via the same email.



ANNEX

Please note: The research grant cannot be utilized for the salary of tenure-track faculty members.

The research budget should be formulated subject to the following limitations:

1. Stipends/Scholarships:
 - a. Scholarships to graduate students (including post-doctoral): at least 35%
 - b. Salaries for researchers and technical personnel: up to 65%.
2. Travel expenses (in Israel and abroad): up to 10%.
3. Hosting foreign researchers in Israel: up to 7.5%.
4. Research Equipment: up to 10%.
5. Equipment and Professional Services up to 10%
6. Events 2.5-10%
7. Teaching: up to 25% and not exceeding four teaching units altogether for a year and all researchers taking part in the research. And will not exceed 40,000 NIS per teaching unit.
8. Proposals with an additional budget, independent of the Israeli government (i.e., not the ISF, Israel's MOST, etc.), will be preferred. The proposed budget should detail the external support and the requested matching from the CCLP.

Sample Budget: 100,000 NIS Funding from CCLP

Item	Amount	Percentage
Scholarships	70,000	70%
Travel Expenses	10,000	10%
Equipment	10,000	10%
Events	10,000	10%
Total CCLP Funding	100,000	100%



המרכז לחקר הסייבר, משפט ומדיניות
The Center for Cyber Law & Policy
المركز لبحث السايبر، السياسة والقانون
אוניברסיטת חיפה UNIVERSITY OF HAIFA



INCD
Israel National
Cyber Directorate