

## University of California Information Security Council (ISC) Charter

The University of California Information Security Council (ISC) is the university-wide collective of Chief Information Security Officers (CISOs) and is chartered by the [UC Chief Information Officer \(CIO\) Council](#). Note: According to [IS-3 Section IV](#), CISOs may also be known as information security officers (ISOs) or campus information security officers at some locations.

### COMMITTEE NAME

University of California Information Security Council (ISC).

### PURPOSE

The primary responsibility of the Information Security Council is to serve as a consulting and advisory body on cybersecurity initiatives to the Systemwide CISO, UC CIO Council, Cyber-Risk Governance Committee (CRGC), Council of Chancellors, President of the UC System, and other UC Leadership. The work of ISC supports UC's mission and drives collaborative cyber security initiatives that yield mutual benefits for multiple locations and the UC system as a whole.

The ISC functions on a consensus-based approach and serves as a closed trust community, fostering an environment of open and inclusive sharing of security information among its members. The ISC supports collaboration and normative practices across the multiple locations and health systems of UC.

### MISSION

To identify, prioritize, sponsor, provide expert advice, and implement programs to enhance cyber resilience of individual locations, the entire UC system, and the greater cyber security community.

### STRUCTURE AND GOVERNANCE

#### ISC

The full ISC is composed of the Chief Information Security Officers (CISOs) from all current UC locations, the executive ISC, and ex-officio members.

#### Co-Chairs

The Co-Chairs offer day-to-day oversight to the ISC and assume their responsibilities in a structured rotation through the voting members according to the sequence shown on the [UC Information Security Council website](#). The tenure of the Co-Chairs spans a period of one year, commencing on July 1st and concluding on June 30th of the subsequent year. In the event a location lacks a permanent voting member, or if a voting member is unable to take on the Co-Chair role and duties for any reason, the existing executive ISC will coordinate with the UC CIO Council member representing that location. In this case, the rotation sequence for that location will be skipped, and the subsequent voting member from the next location will be approached to fulfill the Co-Chair role and associated duties.

## University of California Information Security Council (ISC) Charter

### Subgroups

Subgroups determine their own governing structure and meeting schedule. The standing subgroups are:

- **Executive ISC.** The executive ISC is composed of the ISC Co-Chairs, the Systemwide CISO, and the UC CIO Council Liaison.
- **Campus CISOs.** This subgroup is composed of the CISOs from all current UC campuses, UC Affiliated National Laboratories, UC Agriculture and Natural Resources (ANR), and UC Office of the President (UCOP).
- **Health CISOs.** This subgroup is composed of the CISOs from all current UC health system locations.

### Working Groups

When necessary, the ISC will facilitate the formation of working groups consisting of committee members and individuals from the UC Tech community at large. These working groups will be dedicated to addressing specific tasks with defined objectives and a limited timeline.

### Reporting

The ISC will document its processes, goals, and artifacts to facilitate reporting to relevant parties when necessary. The executive ISC will put forth a group plan and determine what artifacts will be created annually.

## MEMBERSHIP AND PARTICIPATION

Voting and ex-officio members are expected to actively engage in meetings, working groups, general collaboration, open discussions, etc. In cases where a CISO is unable to participate in a required activity, it is expected that they will designate an appropriate non-voting proxy to represent them. Periodically, subject matter experts and representatives from other constituencies, including Privacy; Research Compliance; Export Control; Ethics, Compliance and Audit Services (ECAS); Procurement; IT operations; and others may also be invited to participate in a limited scope of ISC activities. The current list of all members is shown on the UC Information Security Council website.

### Voting Members

All UC location Chief Information Security Officers (CISOs) are expected to serve and participate as voting members. The voting membership only includes the CISOs from all current UC campuses, UC health system locations, UC Affiliated National Laboratories, UC Agriculture and Natural Resources, UC Office of the President, and the Systemwide CISO.

### Ex-Officio Members

These are non-voting members representing ISC strategic partners such as the Liaison to the CIO Council, Systemwide Privacy & Compliance, and the supporting team from the systemwide information security office. Ex-officios support the ISC by facilitating communication with other UC committees and advocating to the UC CIO Council and Executive Leadership across UC. A list of current ex-officio members is maintained on the UC Information Security Council website.

### Voting

Voting within the ISC can occur either during live regularly scheduled meetings or through off-line electronic means. A quorum, which constitutes the necessary participation of two-thirds of the voting members, is required to proceed with voting on an action. An action is considered passed when a majority vote of 51% or more is obtained from the quorum. The votes of each member will be

documented and securely stored for reporting purposes and historical reference.

## **MEETINGS**

### **ISC**

The full ISC convenes at least monthly. At least once per year, the full ISC meets in person instead to allow for extended agendas and to foster stronger connections and engagement between all parties.

### **Subgroups**

ISC subgroups meet separately on a regular basis as determined by each subgroup.