Information Risk Governance Committee Charter

Mission

The Information Risk Governance Committee (IRGC) provides the campus framework for institutional governance of information risk. Information risk includes, but is not limited to, the broad categories of:

- **Autonomy Privacy** – ability of individuals to conduct activities without observation;
- **Information Security** – protection of all information and information infrastructure;
- **Information Privacy** – appropriate protection, use, and dissemination of information about individuals; and
- **Balancing Process** – for the sometimes-conflicting interests of Autonomy Privacy and Information Security.

IRGC is charged by the Compliance, Accountability, Risk and Ethics (CARE) committee to make recommendations on campus information risk issues. These recommendations are campus policy that sets campus information risk tolerances. IGRC's broad membership allows for evaluation of impact on recommended risk management policies across the full diversity of campus activities.

While IRGC will, of necessity, deal with topics that touch on technology, the primary focus of IRGC is information risk as viewed through decidedly non-technical lenses, ranging from alignment with campus values to reviewing the cost-benefit analysis of proposed policy. When technical depth is required, IRGC is supported and advised by the Campus Information Security and Privacy (CISPC) committee, a campus representative group of information technology practitioners.

Decision Domains

- The scope of IRGC information risk management policies is ultimately campuswide, once proposed policy has been approved through usual channels.
- IRGC reviews and decides on exception requests to information risk management policies. This authority may be delegated to the Chief Information Security Officer (CISO) or Chief Privacy Officer (CPO).
- IRGC committee executive sponsors and co-chairs may escalate emergency and very high-impact decisions on exception requests to CARE.
- IRGC reviews the campus information security and privacy programs to ensure adequate transparency on how personal information is protected, what data is collected about electronic activities of individuals, and how such data is used.

IRGC decision-making scope includes:

Management Oversight

- Authorization and oversight of campus information security and privacy strategy as proposed by management to address pertinent changes in laws, regulations, policies, threat landscape, technology environment, and campus information usage, as well as gaps in current campus information risk posture.
- Definition of management reporting requirements for information security and information privacy programs (e.g., for approved data collection programs and delegated authority).

Policy

- Approval of privacy and information security policies and standards, including evaluation of risks as well as costs and benefits of mitigation, considering workload impact across campus. Following IRGC approval, information security and privacy policies are referred to the campus Compliance and Enterprise Risk Committee (CERC) for formal authorization.
- Interpretation and application of campus and UC policy, and adjudication of conflicts between campus initiatives, accepted best practices, and regulatory compliance requirements, including approval or denial of systematic or incident-specific UC Electronic Communications Policy (ECP) violations.
- Escalation and/or approval of issues that do not conform to campus information security and privacy practices, e.g., vendor terms and conditions, contracts, and services incompatible with ECP provisions.

Information Risk Threshold Setting

- Recommends prioritization of resources and determination of campus response to address information risk situations.
- Authorization of protocols for handling information security and privacy policy exception requests, appeals, and escalations, e.g., thresholds for delegation to management.
- Handling of exception appeals and non-compliance regarding minimum security standards and policy, including decisions on whether the presenting risk warrants removal of the non-compliant systems from the network or removal of institutional data from the non-compliant systems, and adoption and delegation of procedures for handling common non-compliance issues.

Areas Of Focus

The committee is charged with campus governance in the following information risk areas *(definitions draw from the UC Privacy and Information Security Steering Committee Report, January 2013):*

Autonomy Privacy

Ability of individuals to conduct activities without concern of or actual observation

Autonomy privacy is an underpinning of academic freedom and is related to concepts such as the First Amendment's freedom of association, anonymity, and the monitoring of behavior; for example, by identifying with whom an individual corresponds or by building a profile of an individual through data mining. Autonomy privacy also encompasses records created by the individual such as research data, working drafts of research findings, communications of ideas, and opinions. It goes beyond the scope of (electronic) information and into the physical world when we speak of direct observation of individuals.

Information Security

Protection of all information and information infrastructure

Information security supports the protection of information resources from threats that could compromise the confidentiality, integrity, and availability of those resources. Information resources include both infrastructure (such as computers and networks) and information (whether or not it is related to individuals). Information security supports, and is essential to, autonomy and information privacy.

Information Privacy

Appropriate protection, use, and dissemination of information about individuals

Information privacy is about the management of information about individuals. It encompasses an individual's interest in controlling or significantly influencing the handling of information about him or herself, whether it is an academic, medical, financial, or other record AND the institution's responsibility as custodian of an individual's information to protect that information.

Balancing Process

Weighing Autonomy Privacy and Information Security interests

The Privacy Balancing Process is a tool that applies the UC Privacy Values and Principles to adjudicate between competing values, obligations and interests of the University when no statutory provision, common law, or University policy is directly applicable. The balancing process rests on the acknowledgement that protecting autonomy privacy depends both on protecting information privacy and on ensuring information security.

Sponsorship

- The Executive Sponsors for IRGC are UC Berkeley's Chief Ethics, Risk and Compliance Officer and Chief Information Officer.
- IRGC reports regularly through the Compliance and Enterprise Risk Committee (CERC) to CARE.

Membership

- Committee membership is designed to be fully representative of the campus.
- Members are expected to be knowledgeable about campus culture regarding privacy, freedom of inquiry, and institutional risk tolerance.
- Each control unit executive must grant his or her IRGC appointees the authority to represent the views and priorities of their respective areas, and make information risk recommendations for the campus community.
- Subject matter experts may be invited by the IRGC co-chairs to speak on specific topics as required
- IRGC co-chairs will recruit members for CISPC from the campus, acknowledging the recommendations of each IRGC appointee.

Procedures

- **Meeting frequency** – Monthly: the committee will determine modifications to the schedule based on needs related to current activities.
- **Meeting structure** – The chairs or a designee will collect agenda items and circulate agendas in advance of each meeting to ensure informed discussion of scheduled topics.
- **Reporting** – The chairs will report on decisions and raise issues and recommendations to CERC and/or CARE and the Information Technology Executive Committee (ITEC), as necessary. Events of critical and immediate threat to the campus will be raised directly to the Crisis Management Team (CMT).
- **Documentation of proceedings** – All meetings shall have notes of discussions and action items.
- **Voting** – Quorum is 70% of voting members; one vote per person.
- **Sub-Committees** – Sub-committees may be established to provide campus oversight on specific compliance topics, such as HIPAA and PCI compliance requirements and establishment of annual attestation cycles.
- **Working Groups** – Smaller working groups bring together subject matter experts to study particular topics in depth, prepare reports, and make recommendations to IRGC. Working groups are appointed ad hoc for a finite term and can be comprised of both IRGC and non-IRGC members.

With these guidelines as a basis, the committee will determine its need for other operational procedures.