OCIP
ONTARIO
COLLABORATIVE
INNOVATION
PLATFORM

OCIP Security

eCampusOntario supports our member institutions to engage in partnerships to support research, work-integrated learning and micro-credentials through our platforms and programs such as OCIP. Currently, we support Ontario-based companies to register on OCIP to find a partner to address a research and innovation challenge. We require companies to be registered Canadian businesses with a business number in order to access the system. eCampusOntario does not screen companies over and above requiring a Canadian business number.

Security is important, and we are aware of the importance of ensuring that potentially hostile state and non-state actors are not able to use platforms such as OCIP to gain unfair competitive advantages over Canadian companies and higher education institutions. We are aware that some information about research facilities may be sensitive information, even if this information is public or published elsewhere. Some members of eCampusOntario choose to use a generic address for research facilities as one way to address this.

Within OCIP there is protection of data built into the design of the system. Data are available only to those who should have access to it; OCIP roles have been designed to ensure data integrity along the following parameters: Access Control, Data Visibility, including Visibility of Innovation Challenges.

Access Control ensures only the right people have access to only the information they need for their function. The OCIP system uses secure user authentication and authorization:

- User Authentication
  Access to the OCIP Portal is only granted to staff from a Participant organization that authenticate using a valid User ID and password. Three categories of Users can be defined: OCIP staff, HEI staff, and Client staff.

- User Authorization
  OCIP uses role-based authorization control (RBAC) to control which Users are allowed access to what functionality. The following Roles are currently defined:
  - OCIP Roles: OCIP Administrator, OCIP Manager, OCIP Project Coordinator, OCIP Funding Administrator, and OCIP Analyst.
  - HEI Roles: HEI Administrator, HEI Manager, HEI Resources Manager, HEI Project Coordinator, HEI Collaborator, and HEI Analyst.
  - Client Roles: Client Administrator, Client Manager, and Client Project Coordinator.

HEI Data Visibility enables each HEI the ability to control how widely available is their information within the OCIP system, by selecting the visibility level for its Academic Units, Facilities, and Research Resources (Equipment and Experts). Four visibility levels are available to indicate who can see the information about this HEI:

- Internal to HEI: only users from this HEI can see it.
- Visible to OCIP Staff: only users with OCIP roles can see it.
- Searchable in OCIP: any logged in user may see it as a search result.
- Public: anybody can see it, including unauthenticated users and external applications.

Visibility of innovation challenges is as follows:

- Client side: visible in full only to portal users created by the Client Admin and assigned the roles of Client Manager and Client Project Coordinator (i.e., only trusted Client users).
- Visible in full only to OCIP users created by the OCIP Administrator and assigned the role of OCIP Manager.
- Partially visible (in a shortened Summary page) to HEI Experts invited to Express Interest or prepare a Scope of Work.

We are open to discussing ways we can work together to bolster confidence in our members in supporting new businesses to find research partners in Ontario.

The technical infrastructure of OCIP is built with security in mind.

- OCIP uses computer-assisted matching to link project requestors to HEI expertise and facilities, and funding programs. AI (Cognitive Search) is used for the SR&ED, NAICS and UNSPSC classification searches.
- OCIP is a single-tenant web application running in the Microsoft Azure cloud, built using commercially available industry standard tools: ASP .Net MVC, C# middle-tier and back-end, and user interface built with Telerik Kendo, JavaScript, HTML5, and CSS3.
- The system uses Platform-as-a-Service (PaaS) components of the Azure cloud, such as Azure SQL, AppService, Storage Tables and Blobs, Key Vault, WebJobs, Queues, as well as Twilio's SendGrid cloud messaging service for email delivery. Semantic-aware Smart Search features leverage AI-powered Azure Cognitive Search.
- External (read) access to OCIP data may be securely provided via a REST API that returns encrypted JSON responses that can be easily integrated into Partner websites and applications.
- The OCIP system is primarily deployed in the Toronto datacenter of the Canada Central Azure region, with automatic replication to the Québec City datacenter of the Canada East region. This deployment approach minimizes cross-border data flows and residency concerns, while providing geographical redundancy.

For Informational Purposes Only. Any and all information provided in this document is for informationalpurposes only and is not to be relied upon as a guarantee, warranty or covenant of any kind, and is not guaranteed to be accurate, complete, reliable, current or error-free, and OCIP assumes no liability in connection with this document.