Mitacs Commitment Regarding Confidential Information from Program Participants

Mitacs is committed to protecting and appropriately managing confidential information provided to us by those applying to participate in our programs. This Commitment Regarding Confidential Information lets you know how we ensure your confidential information is handled appropriately.

NOTE THAT we treat **every** application to our programs with discretion, and staff may not share the information in proposals, except for information identified as being public in the proposal template, with few exceptions (such as providing information to our government funders). This is our normal course of business. In addition, we ensure that third-party peer reviewers agree to keep the information in any application confidential before they have access to the application.

Of course, all applicants and signatories have access to the information within the application, and Mitacs cannot control what the applicants do with the information outside of submitting the application to Mitacs.

Situations in which potential applicants are providing us with information that has a special value because of its confidential nature (often called proprietary or trade secret information) require special handling; under these circumstances, Mitacs must exercise a higher level of care and control of the information. This Commitment defines confidential information and describes how Mitacs manages such information.

1. What is Confidential Information?

Confidential Information is generally information in any format or medium relating to the business and management of a company or organization, that includes proprietary and/or trade secret information and accounting records, such as products, processes, technology, software, business operations information, client lists, technical and engineering data, technical concepts, test data and test results, the status and details of research and development of products and services, and information regarding acquiring, protecting, enforcing and licensing proprietary rights (including patents and copyrights), **that is identified to Mitacs as being confidential**. Note that this is a general definition; a confidentiality or non-disclosure agreement (NDA), which must be signed before Mitacs takes possession of confidential information, will contain a definition that takes precedence over the definition in this policy.

Confidential Information will not include information that:

- is generally known in the industrial sector;
- is now or subsequently becomes generally available to the public through no wrongful act or omission by Mitacs;
- Mitacs rightfully had in its possession prior to receiving the Confidential Information;
- Mitacs rightfully obtains from a third party who has the right to transfer or disclose it.

2. When will Mitacs accept Confidential Information?

Mitacs takes the protection of Confidential Information seriously, and therefore limits the situations in which we will accept or have access to Confidential Information. Currently, none of our systems are

certified for security (such as being PCI or ISO27001 compliant), so we reduce the risk as much as possible through limiting the Confidential Information in our systems.

Under the following circumstances, we can accept or be granted access to Confidential Information (contingent on certain requirements, including the signing of an appropriate NDA, discussed here and in the following sections):

- During discussions with organizations to determine the feasibility of a Mitacs project and to enable identifying potential project participants, we can be provided access to electronic versions of Confidential Information. The Confidential Information must be identified as such. Any hard copies of Confidential Information must be provided to Mitacs staff on site at your organization and collected before staff leave. NDAs must be signed before staff have any access to Confidential Information.
- We will not generally accept Confidential Information in any program applications. The applications must go to third-party peer reviewers and the information is also seen by the university Office of Research Services or its equivalent and all participating professors, students and companies, and potentially support staff as well, so should not contain sensitive information. However, when the fact of your organization working on the project must not be disclosed publicly and/or must not be disclosed to third-party peer reviewers, we can ensure that the company name is removed from the application before it goes for third-party review and ensure it does not go on our website. (Note that we are generally expected to include company names in reports to our government funders, who may make the reports public.)

Any exceptions to these circumstances must be negotiated between your organization and Mitacs. Exceptions will only be considered when the project or partnership is deemed to be of significant strategic value to Mitacs. Depending on the circumstances, exceptions may require the implementation of new procedures or setups, which may delay application submissions and/or reviews and approvals.

3. Why is it important for us to have a non-disclosure agreement?

Confidential Information can have significant value. It is therefore very important that there be a mutual understanding of how that information will be handled once it is provided to Mitacs. Potential applicants should have confidence that we are treating the information with due care, but should also understand that we share information in applications with peer reviewers and funders, and that we are not responsible for information shared among the postsecondary institution and/or other participants in a project. Similarly, applicants should understand that Mitacs's system security is appropriate for us: a not-for-profit whose role is to bring together businesses and academia; we do not have high-value proprietary or trade secret information of our own to protect. The responsibilities of both Mitacs and the provider of Confidential Information need to be documented and agreed to, and a non-disclosure agreement (NDA) (or confidentiality agreement, or proprietary information agreement) will do this. (Mitacs has an NDA template that can be used.) Any NDA must be reviewed by the appropriate party at Mitacs prior to signing, as part of our due diligence; negotiation of terms may be required.

4. How does Mitacs manage and protect confidential information?

At Mitacs, we take responsibility for the Confidential Information in our possession.

Our Chief Privacy Officer (CPO) is accountable for compliance with the Confidentiality Commitment and our confidentiality policies. The CPO may delegate day-to-day responsibility for the administration of the policy to the Director, Risk & Compliance.

All staff to whom Confidential Information is provided are responsible for handling and managing the information in accordance with this Commitment, our confidentiality policies, and with any NDA under which the information was provided. Confidential Information is stored such that only those with a business need to know can have access.