THE UNIVERSITY OF BRITISH COLUMBIA

Guidelines for Telecommuting
Temporary Work from Home Arrangements - COVID-19

Introduction and General Principles

A temporary work from home arrangement is the ability to work off-site for a temporary period of time while social distancing measures are in place due to the COVID -19 pandemic. The purpose of these guidelines is to provide the fundamental elements required for this kind of temporary work arrangement to be successful, and the processes to follow during this arrangement.

Due to the number of staff employed by the University, their various roles and work arrangements, it is impossible to develop a singular temporary work from home arrangement. Therefore, the details of any such arrangement must be determined at the departmental level. HR, in its stewardship role for workplace practices, is providing a framework that enables consistency of approach and practice across the University.

The following are the fundamental elements of these guidelines:

- These guidelines apply to all employees in a temporary work from home arrangement.
- While some jobs and positions will be suitable for a temporary work from home arrangement, not every job or position will be.
- Temporary work from home arrangements will be approved on a case-by-case basis as outlined below.
- Except as expressly agreed between the Department and the employee, this arrangement does not change the terms and conditions of employment for the employee. For purposes of certainty, all existing terms and conditions of employment as set out in the appropriate Collective Agreement, Agreement or Handbook will continue to apply.

Approval of Temporary Work from Home Arrangements

Approval of a temporary work from home arrangement is in the sole discretion of the applicable manager, research lead, or principal investigator, approved on a case-by-case basis.

Workspace, Equipment and Protection of Proprietary and Other Information

Employees approved for a temporary work from home arrangement are responsible for maintaining a suitable and secure off-site workspace at their own expense.

The off-site workspace will be considered an extension of the University's workplace and therefore will be subject to and governed by applicable Workers' Compensation legislation and WorkSafe B.C. Employees will be expected to comply with normal reporting requirements for any work-related accident or injury.

Employees will be responsible for the safe and secure handling of all proprietary and other information taken off-site or accessed from the off-site location, including but not limited to electronic files saved on home computers. For greater clarity, the security systems and policies established by the Department

and the University policies will continue to apply. Employees should review Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems and Information Security Standard #06

The use of UBC supplied and owned computers/laptops are preferred for temporary work from home arrangements. This may take the form of laptops permanently assigned to an employee as their work computer, a laptop from a pool of department laptops which is returned when not in use, or a UBC computer taken home and left at home. It is also possible to use your home personal computer for a temporary work from home arrangement. Your manager, research lead, or principal investigator will assess your needs and approve either the use of a portable workstation or your personal computer. This decision will be recorded by the manager, research lead, or principal investigator. If the department is providing a laptop or other device for a temporary work from home arrangement, the assignment of the device will be logged by the department and you are responsible for returning the device at the end of the temporary work from home arrangement.

The department will provide a checklist of minimum security requirements which will include: anti-virus and anti-malware software installed, regular full-computer virus scans, cabled or hard wired connection to a router or wireless that is password protected, and restricted use by non-UBC individuals. Other considerations include:

- Refrain from using email to transfer data to yourself
- Use USB storage devices that require a password
- When connecting to UBC from home, use a VPN connection
- Avoid CDs and DVDs as they can be lost or copied
- Ensure laptops are password protected so data can't be easily accessed if the laptop is lost or stolen
- Ensure all hard drives and other storage media are encrypted
- Remove information from laptop once it is no longer in use

Employees will continue to be bound by the Freedom of Information and Protection of Privacy Act of British Columbia and any other applicable legislation.