Executive Mandate for Minimum Cybersecurity Controls for accessing UBC Electronic Information and Systems

There is currently a significant increase in the volume and sophistication of cyber attacks specifically targeting universities and healthcare research facilities. We are receiving frequent notifications from government agencies, such as the Canadian Centre for Cyber Security and other reporting agencies, that the number of attacks is surging. These attackers are using new tactics and techniques designed to exploit confusion surrounding Covid-19. The nature of the attacks is often such that the traditional anti-malware and blocking techniques are not sufficient to protect institutional servers, computers and information.

To respond to the increased risk of attacks, combined with the risk resulting from thousands of faculty and staff working from home, increased cybersecurity controls must be implemented on all servers and computers accessing, processing or storing Medium Risk, High Risk, or Very High Risk information, as those terms have been defined in Information Security Standard #01.

The UBC Executive is mandating that:

1. Anti-malware and Endpoint Detection and Response software approved by UBC Cybersecurity be installed on all UBC servers that access, process, or store Medium Risk, High Risk, or Very High Risk information;

2. Anti-malware and Endpoint Detection and Response software approved by UBC Cybersecurity be installed on all UBC-owned faculty, staff, and research computers that access, process, or store significant amounts of Medium Risk, High Risk, or Very High Risk information; and

3. Encryption must be enabled, and current anti-malware software be installed on personally-owned computers used for accessing UBC systems and information. There are many options for your choice of current anti-malware, including the installation of UBC-approved software at no cost. Details about the various options are available on the UBC Privacy Matters website at hxxps://privacymatters.ubc.ca (*UBC does not put clickable links in Cybersecurity communications. Please copy and paste the URL, substituting “https” for “hxxps”, into your browser.)

Complete information about whether you are affected by these requirements, including a copy of Information Security Standard #01, is posted on the UBC Privacy Matters website. The website also outlines the various support models available for faculty, staff and researchers.

It is understood that we are in difficult times with respect to our COVID-19 response, and that access to many servers and computers at UBC has been curtailed as a result of the work-from-home situation. It is recognized that it may not be possible to immediately comply with this mandate as many servers and computers will require physical access. **It is neither necessary nor recommended to deploy the new minimum cybersecurity controls at this time to devices that require physical access on campus. These devices can be updated once regular campus operations resume.**

There remains, however, an urgent requirement to deploy the new minimum cybersecurity controls to devices that can be updated remotely. For some, these updates will take a few minutes and for others it may take weeks or longer to determine the optimal deployment plan, but in any case it is important to move as quickly as possible in order to assure that UBC information is properly protected.