Ensure that the appropriate Endpoint security is in place for all servers, desktops and laptops. This includes personal devices that are used for anything related to UBC Research and UBC Business, especially email. Details about which technologies to use, and how to know that they are properly installed can be found on the Increased Security Controls page from the Privacy Matters @ UBC website. There you will find specific information for both UBC owned devices and personally owned devices.

Verify encryption is in place for all applicable devices and systems.

Enroll your team in self-phishing training. If your team is not yet receiving regular self-phishing messages, speak to your supervisor about contacting the Cybersecurity team to enroll.

If research data is being stored on servers that are internet accessible, those servers need to be registered with UBC Cybersecurity in order for them to receive routine vulnerability scanning. Further information regarding vulnerability scanning can be found on the Cybersecurity Confidential Communications website.

Ensure all research data is properly and regularly backed up.

Review information regarding ransomware on the Privacy Matters @ UBC website.