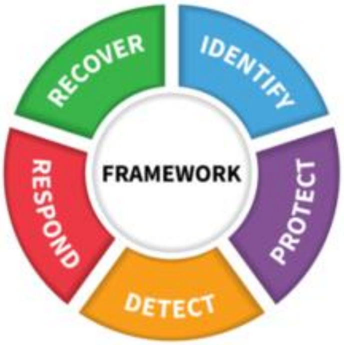
Schedule 3 - A Cybersecurity Guide for NCC Ultimate Recipients

This guide is intended to provide the NCC's ultimate recipients sources and a list of actionable steps to secure their project's people, data, intellectual property, and processes.

1. Sources and recommendations for standard adoption

- Cybersecurity guidance
- Safeguarding your research
- General Information on Research Security
- Guidelines and Tools to Implement Research Security
- What steps can you take to protect your research? (science.gc.ca)
- National Security Guidelines for Research Partnerships
- Canadian Centre for Cyber Security: Top 10 IT security actions
- The top 18 CIS Critical Security Controls
- NIST SP 800-171 - Protecting Controlled Unclassified Information in Non federal Systems and Organizations
- NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations

2. Actionable guide



A cybersecurity framework, e.g., NIST cybersecurity framework, consists of 5 major functions: Identify, Protect, Detect, Respond and Recover. A robust cybersecurity and privacy plan for your project can only be possible when all 5 functions are considered. We encourage the project's principal investigators to review the NIST or a similar framework before implementing a cybersecurity plan for their projects. The major tips and best practices to safeguard project team, research results, data and IP are:

1. Secure your project by design!
   When planning your project and milestones, include cybersecurity goals and objectives at the same time. For example, (1) for the network assets, identify the need for multifactor authentication at the early stage and implement it as early as possible, (2) implement a robust access control, minimize users access privileges, and restrict project members from installing software on their/project devices without authorization; and (3) define incident management role and responsibilities and design a robust recovery plan, to name a few.

2. Establish and enforce a security policy
   This includes educating all project team members regarding risky practices such as sharing passwords and regulating what mobile devices they can use.

3. Install security tools
   Use trusted anti-virus and anti-malware tools and technology to shield and protect your computers, routers, switches, and smart devices. You need to install this software on each device used in the project. The tools analyze traffic and block employees from accessing malicious sites. They add a cost-effective and low-maintenance layer to your project's cybersecurity footprint. Check numerous online reviews to decide on the tools for your project.

4. Data Encryption
   Encrypt sensitive project and personal information on all devices. Ideally, use operating systems that offer encryption in addition to third-party cloud-based solutions.

5. Virtual Private Networks (VPN)
   Adopt a secure VPN, which encrypts data and changes the location and IP address. This is necessary when your project team members are working remotely and require accessing the project's IT infrastructure and data.

6. Training and awareness
   The project team members make a perfect target for hackers; in fact the biggest cybersecurity threat to your project is the staff, collaborators and outside users with access to the project assets. Educate the project team about the security aspects of using remote devices, authentication, managing passwords, social engineering, and risk analysis and mitigation. For example, teach them how to look out for phishing emails. Organize regular workshops to refresh their memories and keep them updated on cybersecurity trends. Continuously test project team members' behaviour during the project and their permissions to access the project's assets.

7. Data confidentiality
   Develop and implement a data governance, rights, and confidentiality protocol for the project. If you are using an automated decision-making tool for data-permission preferences, make sure of the quality of the tool and its underlying algorithm.

8. Using open-source code/software
   While open-source software is used extensively to drive innovation, it should be used with extreme caution and only when you know and have addressed their vulnerabilities and are able to mitigate their risks.

9. Update and patch software frequently
   Most software systems are constantly updating not just for efficiency but security as well - make sure your trusted software is up to date by allying all security patches.

10. Backup
    Backups ensure your data is secure, can be quickly recovered, and you pick up where you last left off. A 3-2-1 backup strategy is recommended, which involves having three

copies of your data, two of which are local (but on different devices) and one offsite (i.e., a cloud backup). If possible, encrypt your backups.