TEMPLATE I: CYBERSECURITY POSTURE CHECKLIST

To be completed by the IT department(s) of the Applicant's organization(s).

F. ORGANIZATION'S CURRENT CYBERSECURITY STRUCTURE		
For applications with multiple partners, complete one checklist per organization. Complete all sections as accurately and as completely as possible.		
THE PERSON COMPLETING THIS CHECKLIST		
NAME: ____________________	TITLE: ____________________	EMAIL: ____________________

CYBERSECURITY QUESTIONNAIRE	
CYBERSECURITY MEASURES	**STATUS**
Which of the following are in place in your organization:	
a. Virtual Private Network (VPN) for employees working remotely	Yes
b. Reliable firewall, intrusion detection and prevention system, antivirus, anti-malware and mobile threat management software for detecting and removing viruses, malware, adware, and spyware	Yes
c. Protocol for managing suspicious emails, instant messages, and texts	Yes
d. Remote wiping for laptops and smartphones	Yes
e. Zero trust security model	Yes
f. Network segmentation to implement unique controls and services for each sub-network	Yes
g. Security Information and Event Management (SIEM) device to continuously monitor and track all network activity across all users, devices and applications	Yes
h. Incident response plan to recover promptly and restore critical functions	Yes
i. Insider threat detection and mitigation process	Yes
AUDITS, PLANNING, AND SYSTEMS PROTECTIVE MEASURES	**STATUS**
1. Does your organization follow a set of cybersecurity rules and procedures on its operations to protect its people, assets, IPs, and sensitive data and ensure systems confidentiality, integrity, and availability?	Yes
2. Is your organization using an automated decision-making tool to implement its data governance, rights, and confidentiality protocols?	Yes
3. Has your organization implemented a robust access control mechanism to control and monitor users' access privileges?	Yes

NATIONAL CYBERSECURITY CONSORTIUM
CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

TEMPLATE I: CYBERSECURITY POSTURE CHECKLIST

To be completed by the IT department(s) of the Applicant's organization(s).

4.	Does your organization regularly use audit tools and controls to identify issues and problems?	Yes
5.	Does your organization apply automatic updates and patches to firmware, hardware, software, and operating systems (OS)?	Yes
6.	Does your organization enforce multi-factor authentication (MFA) for accounts and systems?	Yes
7.	Does your organization categorize assets to identify those most critical to your organization's operational functions?	Yes
8.	Does your organization regularly examine the cybersecurity posture of third-party suppliers and supply chain members (Cloud and key outsourced services to ensure appropriate security measures are in place)?	Yes
9.	Has your organization adopted a well-planned backup system?	Yes
10.	Does your organization communicate cybersecurity best practices and advisories to employees?	Yes
11.	Does your organization provide regular security awareness training for employees and third-party project personnel?	Yes
12.	Does your organization have in place a well-articulated recovery plan for interruptions or breaches, especially for critical assets	Yes
13.	Concerning compliance, does your organization ensure that all assets are configured to maximize their safety and in accordance with industry best practices?	Yes
14.	Does this research project involve the use of personal data that could be sensitive?	Yes

ASSETS

1. Provide the list of the project's IT assets.
   a. List the project's physical assets (computers, servers, mobile devices) and the measures in place in your organization to secure them. For example, the measures could include Control Physical Access, Firewalls, NIDS, HIDS, and SIEMS.

b. Cloud and mobile applications and their security measures.

c. Third-party assets (assets housed on other organization servers and networks) and open-source software. How do you address their vulnerabilities and mitigate their risks?