Technology Helps is a social enterprise committed to ending technology poverty.

EverSecure for Settlement Sector

IRCC Requirements	EverSecure
I. Privacy Requirements	Privacy Policy development for organizations to address critical aspects of data handling and user privacy, including the types of information collected, methods of collection, and its intended use. It will outline how data is stored and secured, policies on sharing with third parties, and the rights users have regarding their information. The policy will also specify data retention periods, any legal obligations for data sharing, and procedures for notifying users of changes to the policy.
II. Minimum Security Requirements Checklist (MSR) • Technological Security Requirements • Physical Requirements • User Requirements • Organizational Security Policies and Training	Cybersecurity Framework developed for organizations which provides comprehensive approach that covers Technological Security Requirements through risk assessment and protective measures, Physical Requirements by identifying and safeguarding physical assets, User Requirements by setting authentication and authorization policies, and Organizational Security Policies and Training by establishing a culture of security awareness and preparedness.
III. Technological Security Requirements • Firewall • Anti-Virus/Anti-Malware • Networks and Networked Computers • Security Patches • Security Settings • Web-Browser • Password Protection and lock Additional Security Measures • USB Keys and other portable storage devices • Cloud storage services and servers • Wi-fi • Email • Intrusion Detection	CIS Framework Assessment - The Centre for Internet Security (CIS) Controls Assessment offers a comprehensive approach to addressing a wide range of Technological Security Requirements. It provides guidelines for implementing secure firewall configurations, deploying antivirus and anti-malware solutions, and maintaining secure networks and computer systems.
IV. Physical Requirements • Password protection • Printing and Document Handling	Cybersecurity Policies - Tailored cybersecurity to maintain data and asset security in compliance with modern standards and establish a cyber-aware culture. It also includes password management policy and guidelines, which is vital in mitigating unauthorized access and potential data breaches. The Policy Bookshelf accommodates up to 27 policies with most organizations typically opting for a range of 10-15 policies. • Assess established policies and controls • Evaluate compliance and address existing gaps by introducing new

	policies and control or modifying the existing ones • Establish a program to periodically re-evaluate these policies and controls
V. Organizational Security Policies and Training • Training Requirements • Procedures and Policies	Cybersecurity end-user awareness programs and policies play a critical role in enhancing Organizational Security Policies and Training. These initiatives directly address Training Requirements by educating staff on best practices for cybersecurity, such as recognizing phishing attempts, securing passwords, and safely navigating the web. Development of comprehensive cybersecurity policies that align with industry best practices and regulatory requirements. This includes developing policies that are tailored to the organization's specific risks and needs.
VI. Privacy Breaches and Violations • Potential Causes of Privacy Breaches • How to Respond to a Privacy Breach	Cybersecurity Incident Response Plan includes simulation and planning for helping organizations prepare for and respond to cybersecurity incidents, with a dedicated incident response manager assigned to the organization. • Assess current risk landscape in the organizations • Identify structure and types of common incidents such as cyber-attacks, natural disasters, or physical security breaches • Develop a comprehensive incident response plan that outlines the steps to be taken in the event of an incident