Language to Request and Justify Funding for Organizational Security Resources

As adversaries continue to develop advanced methods to target us online and disrupt our work, we must remain vigilant to threats and build our capacity to implement appropriate countermeasures. Targeted threats to our digital and physical security have the potential to negatively impact our organization's ability to achieve primary programmatic goals by endangering our staff, compromising the privacy of sensitive program data, and forcing staff to expend time responding to phishing, malware, and other attacks.

Over the past few years, our organization participated in a community-specific security project. Under this project, our organization underwent a full security audit based on the SAFETAG framework. We received a report on the specific risks identified during the audit, tailored recommendations and implementation strategies to mitigate these risks, as well as funds to implement these recommendations to improve our security. As this project comes to a close, we are exploring other funding opportunities to support our continued prioritization of organizational security.

Continued support for organizational security will provide necessary financial and human resources for us to pursue our programmatic goals more safely and efficiently. The resources outlined below will serve to build our resilience as an organization and allow us to mitigate the digital and physical security risks identified as most critical.

Category	**Item**	**Description**	**Justification**
Personnel	Director/ Manager	• *Drafting, implementing, and reviewing organizational security processes and policies* • *Oversee purchase and installation of new software / hardware* • *Leading staff-wide meetings to introduce security processes / policies and raise awareness around security risks*	• *Budgeting specific time for the lead of an organization to address or review security concerns is essential, as it validates the importance of security and carves out financial resources and time that allow the leader to prioritize the organization's security.*
	IT staff	• *Purchase and install new software / hardware* • *Set up new devices with appropriate security features* • *Attend regular meetings with partner/community organizations to discuss relevant threats and mitigations*	• *Budgeting specific time for an individual or consultant to implement security recommendations or policies ensures there will be an owner or champion within the organization to translate ideas into action. Formalizing this role ensures that*

		• *Training new staff on organizational security policies*
		• *Conducting routine security processes including:*
		  ○ *Password resets*
		  ○ *Virus scanning*
		  ○ *Software updates*
		  ○ *Internet network/Wifi router management*
		  ○ *Printer management*
			digital security will be prioritized regardless of programmatic workload.

Consultants	Physical security experts	• *Identify physical risks to office and programmatic processes, and devise mitigations* • *Prepare report outlining physical risk reduction plan*	• *Physical security concerns - including risks to the safety of staff or the security of sensitive documents in an office - can dramatically hinder programmatic implementation.* • *Many organizations lack internal expertise to identify risks and design mitigations.*
	Digital security experts	• *Identify digital risks to office and programmatic processes, and devise mitigations* • *Prepare report outlining digital risk reduction plan* • *Advise on purchasing / installing licenses, software, and hardware and provide general technical support* • *Evaluate and advise on organizational security policies* • *Provide trainings to organization staff on how to identify and mitigate basic digital attacks* • *Provide trainings to organization staff on how to use relevant privacy and security tools*	• *Many organizations lack internal technical expertise to identify digital risks and design or implement technical mitigations.*
	Website developers	• *Maintain website code/structure to eliminate security vulnerabilities*	• *As the public face of an organization, websites are a common target. Compromised websites have the potential to impact both the organization*

			itself and any visitors from the wider community. ● *Many organizations lack internal capacity to maintain website code. Hiring a web developer with experience with open source platforms such as Wordpress (or sending organization staff to a training) ensures that website vulnerabilities are minimized.* ● *Custom code often must be updated or maintained by a particular individual, oftentimes, only the author of the code. Security professionals recommend open source content management systems, like WordPress, given a community of developers maintain the code, the code is consistently updated, and it is a common platform understood and used by many developers.*
Supplies - software	Software licenses (Operating systems; Word Processors; etc.)	● *Purchase genuine, licensed software that is maintained and includes the latest security updates*	● *Licensed software allows the organization to avoid vulnerabilities found in cracked / unlicensed software, which are often excluded from security support and version update services*
	Antivirus subscription	● *Purchase up-to-date Antivirus subscriptions, software designed to detect and protect against computer viruses*	● *Licensed and up-to-date Antivirus software provides organizations with protection from the latest forms of malware.*
	VPN subscription	● *Purchase VPN subscription to anonymize browsing*	● *Using a VPN to anonymize browsing can limit the ability of threat actors or government agencies to monitor the online activity of staff, preventing the disclosure of sensitive content or geographic locations.*

			• *VPN use is especially important for organization staff when travelling to sensitive locations.* • *VPNs can help journalists and activists to access censored online resources.*
Supplies - Hardware	Laptop / phone	• *Old devices are more difficult to update, and regular updates are critical to fix bugs and security vulnerabilities*	• *Maintaining up-to-date and licensed software is vital for device security. As old devices become incompatible with new software versions, purchasing new hardware is necessary in order to reduce these vulnerabilities.* • *Maintaining separate work and personal devices is important for device and data security.* • *Certain models (such as iPhones) are known to be less vulnerable to malware.*
	NAS servers / SSD / other storage	• *External storage to backup sensitive data will protect against data loss in the event of a security breach*	• *Storing sensitive data - whose compromise may endanger the safety of staff or interviewees - on an external storage system adds an extra layer of protection in the event that an organization's systems are compromised with malware / a physical attack.*
	Uninterrupted power supply	• *Separate power supply will protect sensitive equipment and guarantee continuous CCTV system coverage*	• *A power supply that is separate from the mains ensures that physical security systems - including CCTV, alarms, electronic door locks - continue to operate during loss of power.*
Supplies - other	Door locks / CCTV systems / alarm systems	• *To increase physical security based on risks identified in [threat model]*	• *Guaranteeing the physical safety of staff is the most important foundation of programmatic activities.* • *Organizations which store sensitive data in their office are at higher risk of physical attack,*

			which can be mitigated by security systems.
	Safe, shredders	• *Enables organization to secure and safely dispose of sensitive data*	• *Appropriately disposing of sensitive documents prevents data compromises which may endanger the safety of organization staff or interviewees.*
Website Hosting	Deflect, AWS	• *Purchase hosting service for website that provides protection from DDoS and other common forms of attack*	• *Since websites in the community have been targeted by advanced threat actors, hosting the organization's website on secure and reliable servers which provide DDoS mitigation is an important component of website security.* • *Poorly managed servers can enable adversaries to plant malware, distort webpages, or extract private data such as user accounts.*