RoadMap
Strengthening Organizations. Advancing Social Justice.

WEATHERING THE STORMS

Digital Security Readiness Checklist – Baseline IT systems and practices

This checklist contains baseline, ongoing information systems and technology practices that your organization must already have in place in order to successfully take on a digital security initiative. If you cannot check off more than 75% of the items in the list below, it is recommended you focus on meeting these baselines before proceeding with other digital security work. Even if at 75% or above, be sure to note the unmarked items and make plans to implement them as soon as possible, as not doing so will likely undermine your security efforts.

Readiness Assessment: Do you have these Baseline 8 practices in place?	✔
1. Have regular and adequate technical support provided either by staff assigned via job description or contracted with outside agencies. *If your existing hardware and software are not well supported, introducing new tools and practices will likely meet with significant barriers, as new technologies and tools often demand significant ongoing technical support for proper setup and functioning. There are as many ways to secure technical support as there are organizations. Talking to peer organizations in your area is a good way to find quality help.*	
2. Have a culture of training and learning, including strong technology training and follow-up as part of new staff orientation procedures. *New tools and practices demand end user training. If your organization doesn't have established practices around training, implementing improved and possibly complex secure practices is nearly impossible. Beginning with documentation and training for new hires is a wise first step in this area. Following up with new employees at 30-day intervals will ensure they continue to get the support they need to do their work effectively and securely.*	
3. Have a common and clearly communicated set of information systems that all staff use effectively: Know all the platforms you are using for organizational communications. *If your staff are using personal file-sharing, email, task management, or other accounts without knowledge or guidance from the organization, not only will your efficiency suffer but also the environment becomes impractical to secure. How can you protect things you have no access to at an administrative level or, worse yet, don't even know are in use?*	
4. Have a recurrent line item for technology in your budget. *Security is an ongoing process and will require ongoing investments in computer equipment and software to be effective. Work with your technical support provider to determine an appropriate amount to put into this line item.*	

This product was created by Jonah Silas Sheridan and Lisa Jervis of Information Ecology for RoadMap

Readiness Assessment: Do you have these Baseline 8 practices in place?	✔
5. Provide relatively new and adequately powered computers to all staff *Industry standard best practice is to replace laptops and desktops every 3 to 5 years. Encryption tools use a lot of power and can bring older, inadequately powered computers to a near halt, making some security steps untenable for staff. Money for replacing 1/3 to 1/5 of your computers each year should be part of your recurring technology budgeting.*	
6. Have some baseline non-technical security practices *If you do not control your office space and access to your computers, your other digital security steps can be easily circumvented by walking into your office. Rotate alarm system codes, door codes, wireless network passwords and other sensitive access procedures such as emergency building access when staff leave the organization.*	
7. Make sure the computers and other devices you use, including personal devices tat staff may use to access organizational information, are not compromised by malware, viruses or other intrusive software. As a first step ensure you are running antivirus software on all computers. *Antivirus software for Macs and Windows computers is available to non-profits at a discounted rate through Tech Soup Global (http://techsoup.org). If you haven't been running antivirus software or otherwise aren't sure about the status of your devices, you can have the operating system (OS) on it reinstalled to help guarantee the computer is free of malware and viruses. If reinstalling, use a copy from the OS provider, NOT the computer manufacturer, as manufacturers often bundle dangerous software in their installs. There are other ways in which your device can be compromised that will not be remedied by OS install. If you suspect such an issue, get a new computer and call a security professional.*	
8. Have a disaster recovery plan that includes making regular backups of organizational data that are stored away from your main offices. Do not rely exclusively on third parties to back up and hold your information. *This actually is a digital security practice itself, but straightforward and critical enough that it needs to come before any other digital security steps. Talk to your technical support provider about the status of your backups. Refer to the guide at the following link for ideas on how to improve your disaster preparedness http://www.techsoup.org/disaster-planning-and-recovery.*	

If you have these baseline practices in place, you are ready to improve other practices: See checklists for Email Safety, Password and Authentication Safety, and Public Wireless Network Safety.

Please Note: Although these practices are highly recommended they do not in and of themselves constitute a successful security practice. Information security is an ongoing process of managing risk and no list of procedures is an adequate replacement for a thorough review of what information you are protecting, why and from whom paired with an organizational commitment to shifting operations to mitigate risk. Information Ecology, RoadMap Consulting and Common Counsel are not liable for negative outcomes associated with following these practices.

This product was created by Jonah Silas Sheridan and Lisa Jervis of Information Ecology for RoadMap