INFORMATION TECHNOLOGY SECURITY GUIDE

PROTECTING YOU AND YOUR WORK

MEETING SECURITY STANDARDS

Many comprehensive resources provide guidance on organizational security (see appendix). The standards listed below provide a starting point for building strong safety and security management practices. These standards are not intended to cover all safety and security approaches or contexts, and there may be situations where it is not possible to meet the standards.

These materials are presented are for your information only. Wellspring is not in the business of providing security services, and Wellspring does not represent or warranty that these practices are necessary, sufficient or appropriate for any other organization.

STANDARDS CHECKLISTS

MOBILE PHONE SAFETY

- ○ Always add a password or PIN to your phone.
- ○ Set your phone to lock automatically after one minute without use.
- ○ Set your phone to disable itself after 10 consecutive incorrect password attempts.
- ○ Add your medical id information (emergency contacts, blood type, etc.) to your phone so it is accessible during emergencies from the locked screen.
- ○ Be aware that mobile phone conversations are easily monitored and trackable. Use location services only for emergency apps. If your location could endanger you and others, turn off your phone completely.
- ○ Avoid using SMS (text messaging) for secure information since it can be easily intercepted.
- ○ If sensitive information must be transmitted through mobile services, use a secure app (see the Secure Communications section).
- ○ Give your mobile device a non descript name
- ○ Keep track of your SIM cards, if they were stolen the perpetrator would be able to impersonate you.

PASSWORD BEST PRACTICES

- ○ Creating strong passwords is one of the most important parts of securing your information.
- ○ Turn on 2 factor authentication for all of your accounts that handle sensitive information.
- ○ Passwords should have at least 12 characters and a mixture of letters, numbers, and symbols.
- ○ A good tip is to start with a sentence, remove the spaces, intentionally mispell some of the words, and add numbers and symbols throughout.
- ○ You can consult the 2017 NIST Guidelines on Password Practices for more information.
- ○ Change your passwords frequently, once every 3 months if possible.
- ○ Make sure to password lock all digital devices and never give anyone else your password.

AVOIDING VIRUSES

- ○ Avoid clicking on ads and unknown links.
- ○ Never download and open files from unknown sites or open unknown email attachments.
- ○ Don't use unknown flash drives or discs.
- ○ Avoid opening zipped files since virus scanners may fail scanning these attachments thoroughly.
- ○ Adopt a security awareness training tool and develop practices to train yourself and staff on how to detect phishing emails.

OFFICE SECURITY

- ○ Always put away equipment once you are done with it.
- ○ Lock important computers and server equipment out of sight.
- ○ Emergency medical response procedures are posted in public areas.
- ○ Be aware of people browsing over your shoulder. Minimize other people's exposure to your sensitive content.
- ○ Develop and regularly practice an incident response plan for both physical and cyber security incidents.
- ○ Performance reviews evaluate staff compliance with safety and security regulations.
- ○ Staff breaches in safety and security policies are subject to disciplinary measures

INFORMATION TECHNOLOGY SECURITY GUIDE

PROTECTING YOU AND YOUR WORK

TRAVEL SECURITY

- Keep your devices on you at all times.
- Keep your devices out of sight as much as possible.
- If possible, avoid using devices in open public places, as you never know when someone could be eavesdropping.
- Avoid discussing sensitive topics in front of people you don't know.
- Consult with a travel and risk expert if you have plans to travel to a high risk location.

CLOUD BACKUPS

- Since computer hard drives aren't reliable and can be stolen, always keep a backup of all your files on a reputable site in the cloud.
- If cloud storage isn't possible, use an encrypted flash drive and keep it in a physically secure location.
- Internet-based cloud services are the most reliable for backing up your files. Some of the most common services are Box, Microsoft Office 365, and Google Drive.
- Confirm the website you are using to back up your files has https in the URL address. This ensures the data you are uploading and downloading is encrypted in transit.

WIFI ACCESS

- Wireless access points without the proper security can compromise your network and data.
- Make sure any router you connect to has WPA or WPA2 encryption with a strong password to prevent your traffic from being intercepted.
- If you are creating a wifi access point, consider adding a guest network that is not connected to the main network for added security.
- Always change the default admin password on your business and home routers and wireless access points.

SECURE COMMUNICATION

- We recommend the easy to use Signal mobile app for secure voice and chat via mobile phones.
- Different programs and apps offer different levels of security depending on the encryption they use.
- The most secure tools provide end to end encryption, such as PGP mail, OTR (Off The Record) messaging, and the Signal app.
- Email, phones, and text messages are among the least secure methods of comunication.
- Always choose the most secure tool you can given your current resources.
- In many cases, it is often better to reach out for help insecurely than to not reach out for help at all.
- Use BCC when emailing a distribution list. This helps the reader, since they will not have to scroll down to access the new content. It also hides the other recipients from each other, which is often a security necessity.

APPENDIX

- Catalogue of Publications and DVDs for Human Rights Defenders
- Front Line Handbook for Human Rights Defenders: What Protection can EU and Norwegian Diplomatic Missions Offer?
- Insiste, Resiste, Persiste, Existe: Women Human Rights Defenders' Security Strategies
- New Protection Manual for Human Rights Defender
- Protection Manual for Human Rights Defenders
- Security in a Box: Tools and Tactics for Your Digital Security
- Security Planner - Improve your Online Safety
- Stand Up! Security Guide for Human Rights Defenders in Africa
- Workbook on Security: Practical Steps for Human Rights Defenders at Risk