**Guidelines for the use of personal and work equipment**

**Create secure passwords.** When setting up phones, computers, and tablets ensure your device is using a strong password. More about strong passwords are available below.

**Use biometric passwords when possible.** These include fingerprint readers on phones and some tablets, along with Windows Hello facial recognition for some PCs. Biometric passwords should compliment the use of strong passwords.

**Use the passwords and keycodes.**

* Don’t set your phone or PC’s PIN code to 1111 or 1234 or some other similarly simple code.
* Ensure the password lock activates after 1 minute or better on mobile devices and 10 minutes or better for desktops and laptops. Longer periods of time can allow someone to pick up your device and access security settings, data, and file systems before the lock has a chance to engage.

**Encrypt all your devices.**

* iOS devices are encrypted by default.
* Windows 10 PCs can be encrypted by going to Settings > System > About > Device Encryption.
* On Mac OS, you can enable FileVault by going to System Preferences > Security and Privacy > FileVault.
* On Android, open Settings > Security > Encryption.

**Guidelines for data storage**

**Avoid removable media when possible.** Obviously, our MDTs need DVDs of forensic interviews. But avoid storing sensitive information or files on removable media like flash drives and SD cards where possible because they can be easily dropped, lost, or stolen. When using these devices, ensure they, too, are encrypted.

* On Windows, use BitLocker by going to Settings > System > About > Device Encryption.
* Mac OS will require a flash drive be erased first before encrypting it. To do so, go to Finder > Applications > Utilities > Disk Utility. Insert the flash drive, select the drive, go to the Erase tab and select > Mac OS Extended (Journaled, Encrypted). Note encrypting a drive with Mac OS Journaled will prevent it from working on Windows PCs.

**Data stored in the cloud should use AES 256-bit encryption.** Services that follow these industry-leading protocols include Microsoft’s Exchange services and OneDrive, Dropbox, and Backblaze backup. These services and others will be upfront in their marketing materials about the use of this level of encryption. Couple these services with strong passwords.

**Guidelines for sharing data and information**

**Recognize almost all email is not secure.** Corporate environments using Microsoft’s Azure service have access to encrypted email. But virtually every other service does not. Services like Gmail, Office 365, Yahoo, and other webmail providers offer encrypted connections to their services, but once an email is sent, it is no more secure than a letter in the postal mail. Avoid using email to convey sensitive information like financial data, logins and passwords, and social security numbers that can be used to access other services.

**SMS and cellular/landline voice services are not private.** Technology is accessible to governments and consumers that allow for interception of text messages and voice calls. While unlikely to be compromised, avoid sending sensitive information like login details and personally identifiable information across SMS or voice lines.

**iMessage, FaceTime, and WhatsApp communications are end-to-end encrypted.** This means data is virtually indecipherable from the moment you type or speak it to the moment the recipient receives or hears it. Information is encrypted and transmitted on all devices and in transmission.

**Data retention**

**Store important and even moderately important emails for up to two years.** Email storage is cheap, and services like GSuite (formerly Google Apps for Business), Exchange, and others allow for a lot of email storage, so let’s use it. Storing emails for up to 2 years at a minimum means turnover and new hires can transition in quickly, records are kept and indexed, and digital receipts can be stored long after financial reporting periods have passed.

**Consider a document versioning system.** Document versioning is what it sounds like: a way to store documents such as Word files and Excel sheets in versions as they changed. A document that is started, edited, and re-edited might have three versions to it. Document versioning allows variations in those documents to be stored so you can “roll back” changes.

Mac OS has this built-in with Time Machine. Windows 10 PCs can do this with Windows Backup. Dropbox’s Pro level ($9.99/mo.) supports file versioning for all files stored in Dropbox. These serve as backups in case of file corruption, accidental saves, and overwriting or deleting files, too.

**Backup your devices.** iOS users can use iCloud Backup. Android users can use Google’s built-in Android backup service. Windows 10 PCs can use File Backup to an external hard drive, as well as Mac OS using Time Machine.

PCs and Macs can also benefit from off-site backup solutions like Backblaze, which silently backups all of your files as they exist on their servers. The data is encrypted at all points in between for iCloud and Google backup, as well as Backblaze.

In the case of fire, theft, or building destruction (or even a hardware failure), these services can restore all your files by downloading them. Backblaze can even send a hard drive with files via FedEx Overnight for the cost of the hard disk it ships on.

Consider the 3-2-1 rule: 3 copies of your data on two different media and at least one backup offsite.

**Test these backup methods.** Test and review your services annually or better to ensure they’re running, receiving the latest files, and that the restore points aren’t corrupted.

**Dealing with Government requests and data breaches**

**Gather some initial information first.** Do not immediately email or call compromised individuals until you know that a breach has happened or a request has been made. For example, a missing drive or device may just be momentarily lost.

**Be transparent.** Let impacted people know what you think has most likely happened, what actions you’re taking, and what they should do next. If that means the police are investigating, they should know which agencies and who they can contact. If financial data was compromised, people should be aware to check their bank records and what services they should consider changing their passwords.

**Be trustworthy.** Most people recognize nothing is guaranteed. They will also recognize and appreciate any effort by you to be timely, prompt, courteous, apologetic, and know that you care and you took every possible precaution with their information.

**How to create a secure password**

**Passwords should be 16 characters and alpha-numeric.** A lot of services have tried making passwords “easier” for people over time. But if it’s easy for you, it’s easy for someone else. Most services today still do not require as secure passwords as they should, often opting for 7 or 8 characters with a single digit or symbol. Some services still can’t handle an array of symbols beyond !, @, #, $, %, or &.  
  
Your passwords should be 16 characters minimum, alpha-numeric, and with different cases.

Some examples of weak passwords:

* Mittens1!
* J0hn$HoUSE!
* Coral!ne9!

Each of these is short, use symbols that are predictable and words that are available in a dictionary or are familiar names or places. Some examples of moderately better passwords:

* w7GTskFhSX4
* k0kq31hgo29
* cj4lru9h5

The above passwords are moderately more secure because they are not susceptible to “dictionary attacks”. They are, however, still too short, lack symbols, and in some, case variation. Some examples of strong passwords:

* GCyW=NKzxFKZ7=?8
* j@L3R$7YkakMF9Y=
* -4SD=bZSW!WQPgF9

These passwords are at least 16 characters, use a mix of random symbols, cases, characters, and numbers. They prevent “dictionary attacks” and are mathematically challenging (because of their length) for today’s existing computer processors to decode and generate en masse.

**Use a password manager.** Because passwords are so difficult to remember when secure, and because each service you use should have its unique password, consider using a password manager. Services like LastPass and 1Password are free or cheap, easy to use, store your files in an encrypted file on your device, have mobile and desktop versions, run in your browser to generate and save passwords as you go, and have export options that enable you to change services later.

95% of your data’s safety can be maintained just by using a secure password and common sense precautions..

**Safe usage guidelines**

**Use updated browsers on the web.** Use either Chrome or Firefox on Windows or Macs, Safari on Macs, or Edge on Windows for the most security. All three use modern security standards for handling web traffic, can block suspected malicious traffic, and enable you to use plugins to block ads and other malicious information.

**Watch for SSL/TLS secure tunnel transfer warnings.** Chrome, Edge, Safari, and Firefox each display a similar icon in the far right of the URL bar. This icon indicates information being transmitted over the web page is from unsecured sources. It may not be malicious, but it is calling data from some third party service outside that website’s domain.

This icon is also displayed in modern browsers and indicates a site is using secure connections from your device to the server and points in between. It’s commonly seen with sites using https instead of HTTP in the URL. A site may indicate both “Secure” https connections and have an “insecure mixed content” warning icon at the same time.

Chrome is most useful in this regard as it has begun a year-long process to indicate with text cues “SECURE” and “NOT SECURE” in the browser’s URL bar.

**Discontinue use of devices running Windows XP, Vista, or 7.** Also, stop the use of Mac OS X 10.10 or below. Updates are free, work better on hardware that isn’t more than 3 or 4 years old, and provides much better security.

**Be wary of public WiFi services.** Airports, Starbucks, and other venues may have free WiFI, but it opens your device up to a barrage of possible security risks. Your computer’s name appears on the local network for others to see and your Internet traffic can be seen with modest computer hardware and software. Consider tethering your device to your phone’s cellular LTE connection instead.

**Ensure all devices and software are receiving software updates.** Do not continually delay iOS or Android updates, and download Windows and Mac OS updates within a few weeks of their release. iRecord and other software by third party vendors should be updated regularly. It may be a pain or require a restart or time for you to wait while the software updates, but the security updates are critical. Especially for PC and Mac operating systems.

**Keep your Mac’s Firewall or your PC’s Windows Defender on.** Both services are enabled by default when setting up a new device.

* You can check their status on a Mac in System Preference > Security > Firewall.
* On Windows 10, System Settings > Update and Security > Windows Defender. For PCs, Windows Defender can operate alongside or independently of a third party virus/firewall service like Kaspersky or Norton. With smart usage, you likely do not need a third party service like Norton, McAfee, or Kaspersky. These services can sometimes be overkill for users and reduce the useful functionality of your device or become taxing on the processor.

**Enable a good ad blocker – or two – in your web browser.** Microsoft Edge, Apple Safari, and Google Chrome users should consider installing uBlock and Ghostery. Two services that, together, block almost all web-based ads and tracking cookies. Both are available in the respective Plugin Stores for each browser. uBlock, unlike AdBlock or AdBlock Plus, does not take money from advertisers. Ghostery doesn’t, either, and helps prevent third party ad networks from tracking you across the web, including Facebook. These services are also free and not taxing on a computer’s hardware.

**Website guidelines**

Any CAC’s website is going to serve two primary group of people: the people you serve and the people who serve you. Almost nothing about your site should be designed for you or target you or your staff.

The people you serve are almost always stressed, scared, and are often low-income, live in rural areas, and may have low education. This means they’re going to view your site on lower-powered devices, low-bandwidth connections, and may not read everything with the same appreciation for inclusion and broad strokes as you. This viewer is frequently on a 2-3-year-old phone with a semi-stable LTE connection with a low data cap. This viewer is unlikely to understand or care about terms like “multidisciplinary team”, for example, because it’s not specific. “Police, registered nurses, mental health therapists, and DCS caseworker”, however, is specific. This viewer may also struggle or feel uncomfortable not finding “people like me” on your site.

The people who serve you are your donors. This is a group that may view your website at work from an office PC or a newer, high-powered phone or tablet. This viewer is likely interested in what your CAC does, metrics and measurements, and how you spend money. This person likely has a high-bandwidth connection to the Internet. Alternatively, this person could just as easily be an older citizen of the community, somewhat void of technology, and could eschew online material.

**Make your site responsive.** Responsive websites are sites that can expand and contract to any screen size from phones on up to large desktop displays. Responsive websites are one single site, not a “desktop version” and a “mobile version”.

**Avoid script-heavy resources.** Facebook “like” embeds, social sharing services, and photo sliders are all common site features that almost always dramatically increase page load time and add extra download requirements that eat into data caps.

**Linking to third party sites with for-profit services.** Most people most of the time are going to recognize that clicking a link from your website to another website, so long as they look distinctly different with different branding, logos, images, etc., means they’re on an entirely independent website. The most common scenario is linking to a business that has donated money or a partner organization that provides helpful services to your CAC’s visitors.

If you wouldn’t recommend either to a person standing in your CAC or waiting in your waiting room, don’t mention it on your website, either. Recognize that “helpful links” and other link-exchange style pages are low-value to visitors. If people don’t ask you directly face-to-face, most people will always prefer to search on their own rather than rely on your website for third-party help. And website search engines will always award top rank to those direct providers. If you still need to link to third parties, including a disclaimer in your website’s Terms of Use agreement will cover you from liability.

**Sample website terms of use.** Available for use by CACs to copy/paste from freely at <https://incacs.org/library/>.

**Treat your email list respectfully.** Managing email subscribers requires them to submit or give permission to be on your email list. Sending email to many people (50+) without giving them the option to unsubscribe, showing your name and contact information, and a reminder of how they got on the list is a violation of the federal CANSPAM Act.

**Enable an SSL certificate**. SSL stands for “secure socket layer”, it’s what makes a website go from http to https. SSL certificates start at around $80 a year and enable the “Secure” connection lock/symbol in a user’s browser to indicate the connection from their device to the website is encrypted. While originally for services that take and store sensitive information, Google has started rewarding sites with SSL higher search engine rank and “Secure” banners in Chrome version 56. Starting later in 2017, Chrome will display a “Not Secure” security alert to all websites without it.