IRAP Technical Security Policy

For Staff

May 2019

*For staff, we **require** the following actions:*

1. Use of a strong password on all of your devices and accounts (e.g., Podio, email, Dropbox) that contain sensitive client information. Your password should be at least 12 characters long and not be a single word. Do not reuse passwords across different IRAP accounts. Do not use the same passwords between your IRAP accounts and your personal accounts.

    a. We recommend using a password manager (like Lastpass) to create long random passwords and store them in a secure, convenient way, since you will have a different password for each IRAP-related account.

    b. If you do not create a random password, we recommend a passphrase (advice on picking one), which is easier to remember than a random password.

    c. Of the two above options, the password manager option is preferred.

2. You need explicit approval from the Director of Analytics, Technology, & Automation to use a third-party email client to access your IRAP email, unless that third-party client is Microsoft Outlook. Gmail is IRAP's email provider, so using the Gmail app on your IRAP phone (or accessing Gmail through your computer's web browser) to access your IRAP email means that we are not sharing email credentials and client-sensitive emails with additional parties.

3. Enabling two-step verification for your IRAP email account and Dropbox account. You can make an exception for your own computer/phone by having them "remembered" for 30 days. This means your normal use is rarely impacted, but you are protected against someone hacking your password and logging in from somewhere afield. Please note, when enabling two-step verification for Dropbox, do not use the Safari web browser. It distorts the Settings page in a way that prevents you from seeing the Security options.

4. Among IRAP staff, the use of Signal (apps for iOS and Android) for chatting/texting/voice messaging about anything of substance -- anything regarding clients, lawsuits, policy, etc. (instead of Google Chat, Skype, or WhatsApp). Logistical and non-substantive conversations (e.g., "did you see the latest picture of Nimr?") are fine for Google Chat and Whatsapp.
    a. Here are instructions to install Signal on your computer and as a Google Chrome extension; this allows you to chat on your computer like Google Chat or AIM(!). Also in that link: how to modify notifications.

b. Skype-to-Skype calls and Google Hangout calls are permitted, as that audio is not stored on Skype/Google servers. It is the text, transferred files, and voice messages that would be stored on servers in a way that we find too risky.
c. Although Google Chat and Gmail have similar security levels, we require Signal instead of Google Chat to ensure that as much conversation as possible takes place over channels that are as secure as possible. Text chats, file transfers, and voice messages on Google Chat, Skype, Facebook Messenger, or WhatsApp sit on those companies' servers unencrypted (they *travel* via encrypted channels, though). The risk is that a company's servers get hacked or subpoenaed by a government for the data; then our unencrypted chat messages or files can be viewed. Signal avoids that risk by encrypting the message (and attached files) itself at the sender's device and not decrypting it until the receiver's device; your content is encrypted when it's on their servers, so they cannot comprehend it, nor could a hacker or government.
d. If it is not feasible to have clients use Signal to communicate with you, WhatsApp is an acceptable alternative.
e. Once you get Signal, please add your Signal phone number to this sheet for other IRAPtors to be able to add you as a Signal contact. And please add any staffer's number to your contact list if there is a remote chance that you will communicate them over Signal.

5. On public networks (those outside the office and your home), the use of a Virtual Private Network (VPN) for connecting to the internet to do IRAP work. A VPN is a network that you connect to (with encryption) to access the internet; if someone is monitoring your internet activity (like a nefarious coffee shop owner whose wifi you're using), s/he would see nothing other than the VPN server's IP address that you connect to: no content and no requests for any websites.
    a. We are giving everyone with a @refugeerights.org email access to NordVPN. Since each NordVPN account allows up to 6 devices to use, two people will share a given account (VPN buddies) and can each hook up 3 devices.
    b. You will be given usernames and passwords if you have not already. Once you have these credentials, download NordVPN for your computer(s) here. Good tutorials for installing the program on your computer, regardless of operating system, are here. And a NordVPN app is available for Android (with good tutorial) and iPhones/iPad (with good tutorial).
    c. The linked tutorials above show you how to access settings. One setting that you should change is to enable the "kill switch," which will shut down selected applications (e.g., web browsers) if something happens to the VPN connection to ensure you are not left vulnerable. Some other settings you may be interested in:
        i. you can *turn off* notifications
        ii. you can *turn off* the auto-start of NordVPN (auto-start has the VPN **actively wait** for you to use it, it does not automatically connect to the internet via the VPN)

iii. you can *turn on* the auto-connect feature, so you automatically connect to the internet via the VPN on startup.

d. Once you have the VPN running on your computer, or phone, your web usage (inc. applications like Skype) is protected, as all web traffic now flows through the VPN.

6. When traveling internationally with devices that contain IRAP-sensitive information, follow the rules of the Data Security in Transit document. This will include how you structure your files on your computer, so please do not wait to the last minute before reading that linked document.

7. For phones that contain sensitive IRAP information, encrypt the phone storage with a password at least 12 characters long. Here is a document that explains how this can be done for the phone and any accompanying SD card. This adds a layer of security stronger than the login password in case someone gains physical access to your device.

8. Do not store client-sensitive information on your computer outside of any synced Dropbox folders on your computer.

*For staff concerned about any of the threats below, we **recommend** the following:*

Tapped phone lines:

Do: Avoid communicating sensitive information by phone calls and texts[1]; this extends to using an encrypting app to place a call or send a text to a phone.

How: You ***and*** the person you communicate with should use an app that employs end-to-end encryption (E2EE). Common apps like Skype and WhatsApp do, but if the party tapping the lines has great power, read this. Because of this, we recommend Signal.

Why: Phone networks *themselves* do not encrypt content on them; since anyone with access to the network can access the content, unencrypted content is at risk. E2EE only exists when the sender ***and*** receiver are using a service with E2EE. There are apps (e.g., Skype) that use E2EE and can also call/text phones, but not both at once. When such an app is used to call a phone, the voice is not encrypted when it gets on the phone network (as the person lacking the app would have no means to decrypt it). Good news: when ***both*** parties use an E2EE app, it is secure, even using phone data.

Having your internet activity monitored:

Do: Use the Tor browser in addition to your VPN for web browsing.

[1] By ***phone call***, we refer to a call using the phone itself, not a call made using an app. By ***text***, we refer to a regular SMS/MMS message, not a message sent via an app (e.g., WhatsApp).

How: Download the Tor browser from here; do not install plug-ins (which can reveal your identity). This explains how to use Tor.

Why: The Tor browser uses a routing technique that anonymizes you; it is free for anyone to download, but the routing technique slows web browsing and Tor does not encrypt what is being sent[2]. The use of Tor will slow your web browsing a bit.

General eavesdropping:

Do: Use Signal for all of your sensitive communications. Systems that use end-to-end encryption for the message while in transit (Transport Layer Security), but do not encrypt the message itself are less secure, as explained above. These include Gmail, WhatsApp, Facebook Messenger, Skype. While we will still regularly use Gmail, the other apps must not be used for sensitive text-based (or voice-message-based) communication in-house, and only be used with clients if the client is not willing/able to use Signal.

Note: Most email providers today use Transport Layer Security to encrypt their message for transport, so sending an email from example@gmail.com to example@hotmail.com is encrypted. Emails sent from @refugeerights.org addresses are encrypted. Emails that are sent to/from providers that do not use TLS[3] do not get the security of TLS, and are very vulnerable to eavesdropping.

Governments pressuring tech companies for private information:

Do: Use Signal Private Messenger for calling, sending voice notes, and texting.

How: Download Signal to your phone. Use it as you would WhatsApp.

Why: Signal neither keeps your content/metadata on their servers (e.g., WhatsApp) nor has ever shared customer info with governments (e.g., Skype in China).

External Resources

- The Committee to Protect Journalists has recommended these best practices.

[2] So you'll have to do that yourself by visiting sites with **https://** in the URL rather than **http://**

[3] Known non-TLS providers: hotmail.ru, inbox.com, yahoo.co.jp, zoho.com, cox.net, earthlink.net, mindspring.com, rogers.blackberry.net, rr.com, sprint.blackberry.net