Key Questions/Initial Assessment

The purpose of this document is to outline what we want to learn, and what questions we'll ask to do that, in order to understand how secure your organization is and what extra training/ support is required to bring up to a level of best practice.

1. Threat model: Who and what is at risk?
    a. What kind of information does your organization work with on a daily basis? *Eg. contact info of donors, funders, whistleblowers, survey data, financial/payment information*
    b. What/whom do you think of as the greatest risk to your data? *Eg. Government-sponsored hackers, etc., members of hate groups, former staff/volunteers*
    c. Which threats are you most concerned about? *Eg. Social Engineering, etc, physical loss or breach of data*
    d. What would be the consequence of your data being stolen/breached? *Eg. risk of identity exposure for employees, partners, etc., loss of trust, financial*

2. Data Storage & Sharing
    a. How do you store your data? Encrypted HW (Filevault, etc.), password protected devices, etc.
    b. What kind of external storage do you use? (USB, portable HD, cloud, etc.)
    c. What tools do you use to access your data? *Eg. devices, apps, platforms, etc.*
    d. How do you share files internally and externally? (GDrive, Dropbox, etc.)

3. Communication
    a. Do you use encrypted communication technologies? Email or messaging? (Adium, Signal, PGP, etc.)
    b. Do you have a specific communication policy when communicating with your partners?
    c. Do you have email storage policies such as deleting sensitive emails?

4. Data Security Policy: Do you currently have any data security policy or preventive measure? *Eg. Password policy, etc.*
    a. If yes, can you share it?
        i. Does it apply to everyone accessing organization data?
        ii. How do you implement/enforce it?
        iii. Is it reviewed on a timely basis?
    b. Do you use stronger authentication (2FA) for access to email, social media accounts, other online services?

    c. What is your practice for shared access to data? (i.e. shared accounts, common username & password, individual accounts)
    d. Do you have minimum requirements for personal devices and OS for access to organizational data?
    e. Do you have organizational devices for usage by staff?
        i. How frequently do you update the usage software and security software on your devices?
        ii. Does your organization need/use VPNs?
    f. Do you have regular backups of your sensitive and important data?
        i. How secure are your backups?
    g. How do you manage your domain?
        i. Do you have any security measures in place?
        ii. Do you have a secure site? (SSL certificates)
        iii. Are you worried about or have measures in place to prevent or mitigate DoS and DDoS?

5. Organization Structure:
    a. How many teams does your organization have? How many employees per team? How many volunteers/non paid staff?
    b. Do you have any IT team or person?
    c. Who is in charge of allocating access and training?
    d. Do you have different levels of access to sensitive data for paid and non-paid staff?
    e. What is your process for revoking staff access? (in the event of termination, etc.)

6. Past incidents:
    a. What kind of attacks have you experienced in the past two years?
    b. Please provide an example of a past incident (failed or successful). *Eg. phishing email, etc.*
    c. How was the incident identified?
    d. How the incident was dealt with? *Eg. Account reset, consulting a partner, etc.*

7. What is your timeframe for action?
8. On a scale of 1-10, evaluate your digital security expertise.
9. Is your preference for on-site or remote assistance?