[redacted]

Cyber Incident Response Policy

Before any incident or security breach occurs, **print this policy** and any documents linked in it. If [redacted]'s network is unavailable, you will not be able to access this electronic file. The Chief Information Officer, Chief Legal Counsel, and Chief Operating Officer are responsible for keeping separate hard copies of this policy in their offices.

While adopting and following security best practices for acceptable use of electronic equipment offers significant protection, no policy will ever eliminate the risk of a security breach. The precautions we take against compromised or easily guessed passwords, malware, and phishing attempts only reduce the likelihood. Phones and laptops can be lost, broken, or stolen, and even the best of us let our guard down sometimes. When prevention fails, a fast response is critical to minimizing the damage to [redacted], our clients, our staff, and our volunteers.

If you are accessing the [redacted] network or using [redacted] equipment and you believe that your account or equipment has been compromised, you should:

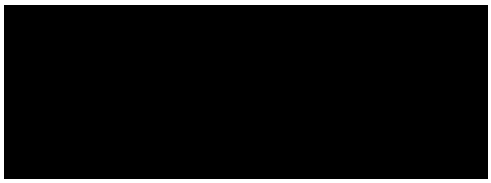
1. Log out of your account,
2. Shut off your electronic device, and
3. Contact Technical Support at [redacted] or [redacted].

Once an incident is reported to the IT staff, the following steps shall be taken by the individuals and their staff identified below within the relevant time periods.

Response	**Lead**	**How soon after incident reported**
Diagnose a breach	Chief Information Officer	As soon as possible
Remove access and secure [redacted] data on equipment and network	Chief Information Officer	As soon as possible
Secure [redacted] physical offices, if necessary	Chief Operating Officer	As soon as possible
Preserve data; remove and preserve any improperly posted data from [redacted] network	Chief Information Officer	Within 1-2 days
Remove and preserve any improperly posted data from public sites	Chief External Relations Officer	Within 1-2 days

[redacted]

Communicate with staff via org chart phone tree, as appropriate.	Chief Executive Officer/Executive Director, Deputy Director, Managers	Within 1-2 days
Gather info from staff who discovered breach; hire a data forensics expert if necessary	Chief Information Officer	Within 1-3 days
Consult with legal counsel who has privacy and data security expertise	Chief Information Officer	Within 1-3 days
Contact cyber insurance provider	Chief Legal Counsel	Within 1-3 days
Notify law enforcement agencies, if appropriate	Chief Legal Counsel	Within 1-3 days
Determine full extent of breach: work with forensics expert if necessary to identify systems, accounts, data and individuals affected (clients, staff, donors, community partners, others); determine whether electronic health information involved.	Chief Information Officer	Within 1-3 days
If the breach involves **electronic health information**, review FTC Health Breach Notification Rule, HIPAA Breach Notification Rule, and applicable forms (see Additional Resources below); provide notice to the FTC, the media, and/or Dept. of Health and Human Services (HHS), as appropriate	Chief Legal Counsel	Within 1-2 weeks
Communicate with media, if necessary	Chief Legal Counsel	Within 1-2 weeks
Coordinate notification to those impacted by breach, pursuant to applicable federal/state law	Chief Information Officer	"without unreasonable delay," so within 1-3 weeks



Develop remediation plan pursuant to applicable federal/state law; repair or replace damaged technology; restore data from backups	Chief Information Officer	Within 2-3 weeks
Debrief with leaders, team members; take steps to improve incident response; update policy as necessary	Executive Director, Deputy Director, Chief Information Officer	Within 3-4 weeks