IslamicFamily Cybersecurity Policy

▼ Table of Contents

Brief

Maintaining the relationships, trust and integrity we have built with community requires us to treat the data we hold as a sacred trust, plan for continuity of service & reduce the impact of cyber incidents.

The purpose of this document is to make it easier to know what *practical* steps to take to build a more secure organization by identifying assets/risks and preventative and reactive measures organizations can take.

How to adapt this document to your needs…

1. Identify what digital assets you have (the list below should help). Digital assets include hardware, passwords, subscriptions, information you store (such as client/supporter contact data), social media, etc.
2. For each asset identify…
    a. Preventative measures you have in place
    b. Steps you need to take
    c. Reactive measures you'd take if the asset were compromised (eg. What would you do if your executive lost all of their sensitive passwords or a staff member's computer was compromised by a malicious agent?)
    d. Identify who's responsible: what training might they & the team need?

Principles

The principles underlying our approach to cybersecurity are…

1. **Technology is an Opportunity**
   We want to facilitate our teams use of tech in a joyful, optimistic and curious way. Tech provides an opportunity to communicate in new ways, improve workflows and bring delight.
2. **Focus on achievement not activities**
   Security is not about busy work, it must focus on measurable proactive steps with discernible results; eg We can't just focus on awareness, we must track the percentage of devices we have that are running up-to-date software.
3. **Prepare/ Prevent**
    a. **Zero trust:** Do not assume trust with digital assets, assume people may lose their computer, be hacked etc.

b. Conduct an annual risk review at the board and management level that includes an internal audit of systems/assets and scenario planning

c. Minimize the amount of doors that can be opened with one account & minimize the number of people with access to admin accounts. *1 key opens only 1 door.*

d. Review/ monitor systems looking for unusual activity

4. **Inform & Rectify**
   Communicate compromises and losses as we learn about them to the people that are impacted by them; clients, team, partners. Second, do our utmost to rectify the damage caused by loss through support (especially for marginalized individuals), connection to resources, revising policy/procedures and apologizing.

5. **Paranoia Undermines Prevention – Be Honest**
   Hostile policies undermine security. We want our teams to feel safe and supported. We do not want them to feel like they are being watched, confined or restricted by policies. Second, we need to be honest and transparent; cybersecurity tools enable surveillance and have the potential to undermine culture and effectiveness. We should adopt an "Honest Security" approach.

   a. A security program should represent our organization's values.

   b. A positive relationship between end-users and the security team is critical.

   c. Trust is the foundation of such a relationship and is demonstrated through informed consent and transparency.

   d. Our detection capabilities should anticipate that end-users will use their company issued devices for personal activities.

   e. When educated and honestly motivated, end-users are capable of making rational and informed decisions about security risks.

Staff Training

All staff must undergo onboarding (& thereafter every two years) training. Training records will be kept in WebHR. Training will include…

1. Creating safe and secure passwords using a password manager (eg Apple's Keychain, 1Password).

2. Using the internet and social media safely. This should include proactive and positive ways to engage on social media. (See: Creating a Personal Voice Plan).
3. Safely using software and apps on workplace devices.
4. How to identify malicious links and phishing emails.

Staff who's roles involve "how" we handle client data must also undergo training on…

5. Obtaining consent. Studying the First Nations principles of ownership, control, access, and possession (OCAP), GDPR, & PIPEDA.
6. Storage of data on devices & the cloud.

Staff whose roles involve building/managing digital products and social media must…

7. Complete the Toronto Metropolitan University: Simply Secure e-learning modules.

Assets & Measures

Data & Managed Assets

Digital Asset	Preventative	Reactive	Who's responsible
Passwords	▸ Keep passwords in a secure wallet and limit access to wallet ▸ Rotate passwords after departure of personnel		Operations

Digital Asset	Preventative	Reactive	Who's responsible
Client Data & Personal Info	▸ Store client data securely and transmit it via encrypted channels to the extent possible ▸ Minimize retention of client data by deleting photos of documents, etc & not storing sensitive items on the cloud ▸ Seek/document proactive consent before recording and sharing information	▸ Inform any clients that may have been impacted by the breach ▸ Offer support w/ identity theft (???)	Innovation Director, Clinical Director, client facing staff
Supporter & Donor Data	▸ Only input payment data via secure methods that do not retain info on the device ▸ Limit full access to DRM (Donor Relationship Management) to Controller, Community Relationships Manager, and senior directors ▸ Provide partial access to DRM (name, contact details, length of relationship) only to those who have completed a security check and signed an oath ///Can we use Bloomerang/FundraiseUp to place calls so that donor contact data doesn't stay on client computers?		Community Relationships Manager, Controller
Access to Subscribers/ Followers	▸ Limit access to SM (Social Media), mailing lists, etc to select staff		Communications Lead

Digital Asset	Preventative	Reactive	Who's responsible
Internal Communication Systems (eg cell access, email, slack)	▸ Inform staff of our communication fall back plan. eg If Slack goes down then email, if GSuite goes down then call your manager, if in doubt come to the office ▸ Maintain a calling tree (What'sApp/ Signal group) with the contact details for staff, board & exec	▸ Send team updates via calling tree / alternative group chat	Operations
GSuite Accounts (misuse or misappropriated via phishing)	▸ Suspend all account access as a part of staff off boarding ▸ Suspend volunteer/board accounts after 6 months of inactivity ▸ Internally practice two-factor authentication with any requests (eg creating a new account for a volunteer should be verified via slack & email).	▸ Inform staff of fallback option should there device be compromised. eg. Visiting office, calling and answering identifying questions ▸ Suspend any accounts acting suspiciously ▸ Remote wipe devices	Operations
Digital Subscriptions	▸ Review all active digital subscriptions monthly via credit card statements and accounts payable ▸ Maintain list of active subscriptions on Notion	▸ Cancel unwanted subscriptions, inform credit card company of unauthorized payments	Operations
Staff Payroll	▸ Limit access to payroll to Controller ▸ Controller to review payroll provider statements ▸ Auditor to review payroll	▸ Have two reviewers of payroll: ED & Controller	Controller Treasurer ED
Finance Systems: Outgoing Payments	▸ Authorize outgoing transactions (EFTs/ etransfers)via 2 modes of communication (eg email & slack) ▸ Require two to authorize any outgoing payments		Controller Treasurer ED

Digital Asset	Preventative	Reactive	Who's responsible
Finance Systems: Incoming Payments	▸ Review any changes to incoming payments and track expected to actual quarterly	/// Do we have controls to monitor if direct payment info changes?	Controller Treasurer ED

Owned Assets

Digital Asset	Preventative	Reactive	Who's responsible
Physical space (Hüb)	▸ Require pledge for accessing our space (door access is not to be shared) ▸ Only provide access to staff, pledge takers ▸ Limit access based on need/ security authorization ▸ Review access logs ▸ Secure wifi with different access for staff & guests		Operations
Physical devices	▸ Install and maintain mobile device management (MDM) software ▸ Apply patches within 14 days ▸ SIM lock all phones via carrier to prevent SIM swap attacks ▸ Monitor staff devices for security threats using MDM ▸ Share monthly update on status of staff devices: how many devices need update/patches, how many threats have been avoided	▸ Wipe any device reported missing	Operations

Digital Asset	Preventative	Reactive	Who's responsible
Internally Developed Apps	▸ Conduct third party audit of app data transmission to verify ETE encryption & security of data. ▸ Third party audit of code(???) for data security? ▸ Implement different types of cybersecurity software that focus on: combatting cybersecurity attacks, like DNS filtering, malware protection, antivirus software, firewalls and email security solutions. In addition, data that lives on computers, smart devices, routers, networks and the cloud need protection software. ▸ Regular cadence of system backups and updates. ▸ Implement guide to ensure personal data protection, password idleness, suspicious emails/urls, and physical security of devices.		Product Manager

External Risks

External Risks	Impact	Prevention	Reaction	Who's responsible

External Risks	Impact	Prevention	Reaction	Who's responsible
Targeted by social media (Doxing, Misinformation, Disinformation)	Overwhelm phones, SMS, email and make communication w/ clients difficult	► Monitor complaints email & hotline for unusual activity ► Maintain accurate information on web & social media	1. **Report** – Attempt to remove problematic content that mentions the organizations through reporting the content. This may need to be coordinated by multiple staff members in order to gain sufficient attention by moderators. 2. **Ignore** – Do not engage with the content if it may lead to increased attention. 3. **Inform** – Prepare and post a response to the content	Communications Manager

External Risks	Impact	Prevention	Reaction	Who's responsible
Vendor Breach (eg. AWS or Google is involved in a data breach)		▸ Maintain list of systems we are dependent on and monitor them for compromises. eg AWS, GSuite, Stripe ▸ Maintain list of systems we use and what systems they are connected to (eg Notion is built on AWS). ▸ Use 1Password monitoring to stay apprised of system compromises.	▸ Inform any stakeholders when breaches occur with our vendors	

References & Acknowledgment

This policy was co-developed with the CIO Strategy Council.

Honest Security

CIO Strategy: Baseline Cyber Security Controls For Small And Medium Organizations

Cybersecure Canada: Employee awareness training plan

Toronto Metropolitan University: Simply Secure e-learning modules

NTEN: Cybersecurity for Nonprofits

National Council for Nonprofits: Cybersecurity for Nonprofits

Ann Lewis: Digital Security Policy Template for Nonprofits

Microsoft: Nonprofit Guidelines for Cybersecurity and Privacy

SANS Institute: Security Awareness