Trusted Family

Information Security Checklist



A simple Google search will yield a host of intimidating data on the state of security. Let it suffice for now to say that IBM puts the global average cost of a data breach in 2024 at USD 4.88 M – a 10% increase over the year prior and the highest total ever.

While it is easy to get swamped by the scope of what needs to be done, or swayed by constantly shifting priorities, there are a few foundational principles key to keeping your state of security primed. If these are routinely reviewed, maintained, and disseminated across key stakeholder groups, an organism as complex as a globally-distributed team can ensure their preparedness for anything untoward.

Here, we propose a simple checklist of such principles. For the more savvy security organization, we encourage you to stay abreast of what's new with respect to these aspects, e.g. how is AI impacting both the attack and defense vectors. For others who might feel "insecure" about the state of their security practice, start with the basics of each principle and revisit routinely with the spirit of continuous improvement. One added advantage that will automatically accrue is that it will keep security front and center for all key stakeholders, keeping them vigilant and proactive on even the whiff of a threat.

1. Create a cyber-aware culture in your family enterprise ecosystem

SECURITY MANAGER

- ○ Appoint someone in charge of information security for your family enterprise & family.

SECURITY ASSESSMENT

- ○ Perform an initial security vulnerability assessment:
  - ☐ Identify where sensitive data is stored, and who has access.
  - ☐ Define control points and indicators guaranteeing safety of data. These should be monitored routinely.
  - ☐ Have a business continuity plan in place that serves as a checklist of actions in case of (suspected) compromise with clear roles and responsibilities.

SECURITY POLICY

- ○ Develop a security policy to create a shared understanding of security priorities and rules across the family enterprise and family.

SECURITY TRAINING

- ○ Conduct a training for staff and family members:
  - ☐ Password security best practices.
  - ☐ What a potential attack looks like, so they know how to recognize them to avoid falling into phishing, malware and ransomware traps.
  - ☐ Social media best practices.

SECURITY CHECKUP

- ○ Organize an annual information security checkup to identify risks and prepare an action plan to address/mitigate the more important risks during the year.

2. Build strong controls around devices and data

STRENGTHEN DEVICE & DATA CONTROLS

- ◯ Create a backup of all necessary business/family information using a trusted cloud-based technology.
- ◯ Enable two factor identification on all devices and accounts that manage sensitive data.
- ◯ Encrypt all of your sensitive data on laptops and mobile devices.
- ◯ Protect your systems by limiting access rights and limiting the number of administrative accounts.
- ◯ Create an email alias where family and staff members can report suspicious activity.
- ◯ Select a VPN provider so that family members and staff members can connect securely from remote locations.
- ◯ Develop policies for guest wifi, so that cannot join the main enterprise network, or networks of family members's homes.
- ◯ Implement a device management tool to make sure all firmware and software remains up to date.
- ◯ Institute a hardware disposal and data destruction policy for different data categories so that such disposal doesn't end up as inadvertent leaks.

Trusted Family

Revolutionize the way your family business operates digitally.

www.trustedfamily.com

©Trusted Family 2025, All rights reserved