CHECKLIST

How cyber secure is your family office?

Cybersecurity threats are growing, and family offices are often targets due to the sensitive data and financial assets they manage. By taking proactive steps, you can reduce your exposure and strengthen your defenses.

Access & Authentication

- [ ] Restrict devices, networks, and systems to authorized users only.
- [ ] Eliminate shared logins and require unique credentials for every user.
- [ ] Enforce strong, unique passwords across all accounts.
- [ ] Enable multi-factor authentication (MFA) wherever possible.

Device & Data Protection

- [ ] Encrypt sensitive files and data both at rest and in transit.
- [ ] Back up critical information securely and regularly.
- [ ] Configure devices to lock automatically after inactivity.
- [ ] Install antivirus/endpoint protection software with automatic updates.

Phishing & Email Security

- [ ] Train family members and staff to recognize phishing attempts.
- [ ] Encourage verification of suspicious messages through alternate channels.
- [ ] Promote a "when in doubt, ask" approach before clicking links or attachments.

Remote Use & Travel

- [ ] Avoid public WiFi for sensitive work and use VPNs for secure connections
- [ ] Download apps only from trusted sources and delete unused apps.
- [ ] Use personal chargers instead of public USB charging stations.
- [ ] Limit access to sensitive applications on mobile devices.

Reporting & Awareness

- [ ] Create clear processes for reporting suspicious emails, errors, or unusual device activity.
- [ ] Engage cybersecurity professionals for regular assessments and guidance.

KAUFMAN ROSSIN