TRUSTED FAMILY

PROTECT YOUR FAMILY'S LEGACY

A Cybersecurity Blueprint for Family Businesses

Proactive cybersecurity is essential for safeguarding your family's assets and reputation.

A Trusted Family platform can play a key role in your security plan.

RANSOMWARE
Encryption of data for ransom

INSIDER THREATS
Employees or family members causing harm

PHISHING
Deceitful emails to steal sensitive information

DATA BREACHES
Unauthorized access to sensitive data

With these types of threats in mind, family businesses and offices should develop a cybersecurity plan that fits your current size and complexity of family and needs.

Developing Your Cybersecurity Blueprint

1 RISK ASSESSMENT

- **Identify assets**
  Determine what information, systems, and assets are critical to the business
- **Threat identification**
  Identify potential threats and vulnerabilities
- **Risk evaluation**
  Assess the likelihood and impact of each threat
- **Prioritization**
  Rank threats based on their potential damage

2 STAKEHOLDER TRAINING

Educate family members and shareholders on cybersecurity best practices

- **Security awareness**
  Educate employees about common cyber threats (phishing, ransomware, social engineering)
- **Password management**
  Teach employees to create strong, unique passwords
- **Data handling**
  Explain how to handle sensitive information
- **Incident reporting**
  Outline procedures for reporting suspicious activities

Trusted Family's Role

A Trusted Family platform can provide a way for you to mitigate potential risks of cyber threats by providing a single, secure method for information to be shared - **on the platform**. Thus, any requests, links and downloads not through the trusted platform would be suspect for your family members.

3 STRONG PASSWORDS

Encourage complex and unique passwords

- **Password policies**
  Implement strong password requirements (length, complexity, uniqueness)
- **Password managers**
  Encourage the use of password management tools
- **Two-factor authentication (2FA)**
  Enable 2FA for critical accounts

Trusted Family's Role

TF 2.0 allows for enabling 2FA for logging in as well as optional security measures (watermarking and download prevention) for the most sensitive of information to be handled appropriately.

4 DATA BACKUP

Schedule regular data backups to prevent data loss

- **Regular backups**
  Implement regular data backup routines
- **Backup storage**
  Store backups securely off-site
- **Backup testing**
  Regularly test backup restoration procedures

Trusted Family's Role

With TF 2.0, your documents and communications are regularly backed up without any additional effort on your part.

5 INCIDENT RESPONSE PLAN

Have a clear plan for handling cyberattacks

- **Incident response team**
  Designate responsible individuals
- **Communication plan**
  Establish procedures for internal and external communication
- **Data recovery procedures**
  Outline steps to restore systems and data
- **Business continuity plan**
  Plan for continued operations during a disruption

6 NETWORK SECURITY

Protect your network with firewalls and intrusion detection systems

- **Firewall**
  Install and maintain a strong firewall
- **Intrusion detection and prevention systems (IDPS)**
  Implement to monitor network traffic
- **Network segmentation**
  Isolate sensitive data and systems
- **Access controls**
  Limit network access to authorized personnel

Trusted Family's Role

TF 2.0 is designed to limit access to those who need access to specific information. As a platform, we also prioritize a secure infrastructure including two-factor authentication, encryption*, daily backups and virus & malware screening.

*For more details on our encryption systems for data in transit, during storage, at rest, and for our backups, see our TF 2.0 Encryption Systems Whitepaper

7 PATCH MANAGEMENT

Keep software and systems up-to-date

- **Software updates**
  Keep operating systems and applications up-to-date
- **Vulnerability management**
  Identify and address software vulnerabilities
- **Patch testing**
  Test patches before deployment to avoid disruptions

Trusted Family's Role

With TF 2.0, you can rest assured your systems are regularly updated with the latest security measures and the platform is regularly tested for vulnerabilities.

AICPA SOC 2 Type II AICPA SOC 3 Type II

PROTECT YOUR FAMILY'S LEGACY WITH A ROBUST CYBERSECURITY PLAN

Contact Trusted Family for a comprehensive solution

www.trustedfamily.com

Remember: This is a general outline, and the specific details of your cybersecurity plan will depend on the size and complexity of your family business. It's essential to regularly review and update your plan to address evolving threats.