Jewelers Mutual®
EST 1913

Technology and Cyber Security Important Considerations

Expectations for Technology Service Providers (Hardware/Software support):

- Set up technology services with the flexibility to transition seamlessly to another partner if service problems or value is not realized.
- Establish clear contractual service level agreements (SLAs) when it comes to issue resolution and service disruptions, including how to hold the vendor accountable for consistent breaches (e.g., invoice credits).
- Establish a primary point of contact with the software vendor and conduct regular business reviews to ensure the relationship is healthy, the software meets your needs, and the vendor is investing in the right areas to support your strategic growth.
- When choosing a solution, make sure to consider all regulatory requirements, especially those related to privacy. Ensure you can be compliant when storing Personally Identifiable Information (PII).
- Keep your hardware and software (including operating systems or firmware on any networking, server or PC equipment) fully supported to ensure you get valuable security updates and functional patches.
- Understand how your data is backed up and protected to ensure the recovery approach and timeline are acceptable.
- Understand how your service provider's security or data protection safeguards are implemented.

Important Data/Cyber Security Considerations:

- Establish a security aware culture and mindset in your organization from the top down
- Establish a plan to respond and recover from a ransomware event
- Establish a relationship with a partner you trust to assist if a security incident occurs
- Train your employees on security awareness
- Ensure appropriate employee access to information
- Establish strong authentication controls, including:
  - Leverage strong passwords
  - Do not share your passwords
  - Do not use generic accounts
  - Utilize passphrases
  - Use multi-factor authentication (Often a cyber insurance requirement)
  - Leverage a password safe to manage sensitive information, like Bitwarden or Dashlane
- Establish strong technical controls
  - Install an anti-malware solution, encrypt your data, and implement a firewall