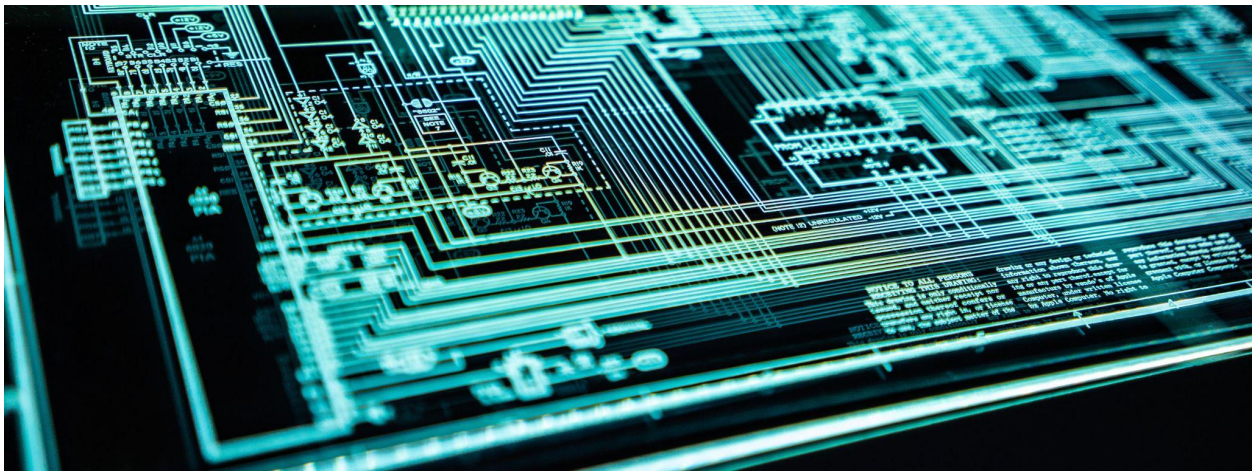
Considerations for Nonprofits in their Partnership Agreements



Introduction

This document will provide guidance to nonprofit organizations, particularly small to midsized NPOs, in their dealings with their for-profit vendors. It is intended to provide a list of issues for NPOs to consider when entering into an agreement with a for-profit partner.

To begin, there are a number of issues — most of which are straightforward and obvious — that any NPO should consider before entering into an agreement with a for-profit entity. Specifically, any contract with a vendor should stipulate that the vendor (consultant) will comply with applicable laws related to privacy and security of consumer data, as well as the nonprofit's own privacy policy. The Vendor should also state they will comply with all applicable federal, state, and local laws, statutes, acts, ordinances, rules, codes and regulations, executive orders and other official releases of or by any government, or any authority, department or agency thereof, in any jurisdiction from or in which the services are provided or received.

Now, here are a number of items the NPO should look for in an agreement with a vendor to ensure a good organizational fit.

1. Disclosure

NPOs should be aware that different states have different notification laws, and the NPO should be aware of those that are applicable to them, particularly in terms of their responsibility to notify their donors. NPOs should look for language addressing how their vendor will inform the NPO of any known or reasonably suspected security breach or unauthorized disclosure of consumer information or confidential information.

2. Data Security

The vendor should be expected to follow best practices to ensure that software used to provide services will not contain vulnerabilities or defects which would allow unauthorized access to, or alteration or destruction of, consumer data.

Specifically, the NPO should ask the vendor to describe the vendor's safeguard system of the NPO's data that it will possess. Accordingly, the vendor should agree to promptly respond to security-related inquiries from the NPO and take all necessary steps to identify, investigate, and resolve security issues to the reasonable satisfaction of the NPO. The NPO should obtain a copy of the vendor's incident response and notification protocol.

3. NPO Ownership

The NPO should retain all rights, title, and interest in and to any materials provided by the NPO to the vendor, such as content, data, as well as all information about the NPO's finances, donors, customers, constituents, and other activities, including without limitation all customer information obtained by the vendor in performing under its contract with the NPO.

Additionally, the vendor should represent and warrant that it is the owner of all rights necessary to perform services and provide the deliverables. Also, the vendor should agree to not infringe, violate, or misappropriate any patents, copyrights, trademarks, trade secrets, or other proprietary or intellectual property rights of any third party.

4. Insurance

The vendor should maintain general liability insurance and errors and omissions insurance policies to cover any and all claims, no matter where made, arising in connection with the contract. The insurance shall be evidenced on certificates of insurance and furnished to the NPO. Many NPOs now require cybersecurity coverage.

5. Resiliency

The NPO should determine the availability of the vendor having a back-up system in the event of an interruption to a mission-critical service. The NPO should discuss with the vendor the need for a Recovery Service Level Agreement (SLA) in terms of how long the vendor's system will be down in the event of an interruption.

6. Compliance and Termination

In the agreement with the vendor, the NPO should have a clear understanding of what constitutes compliance by the vendor with the NPO, as well as the timing and terms as to how the agreement can be terminated.