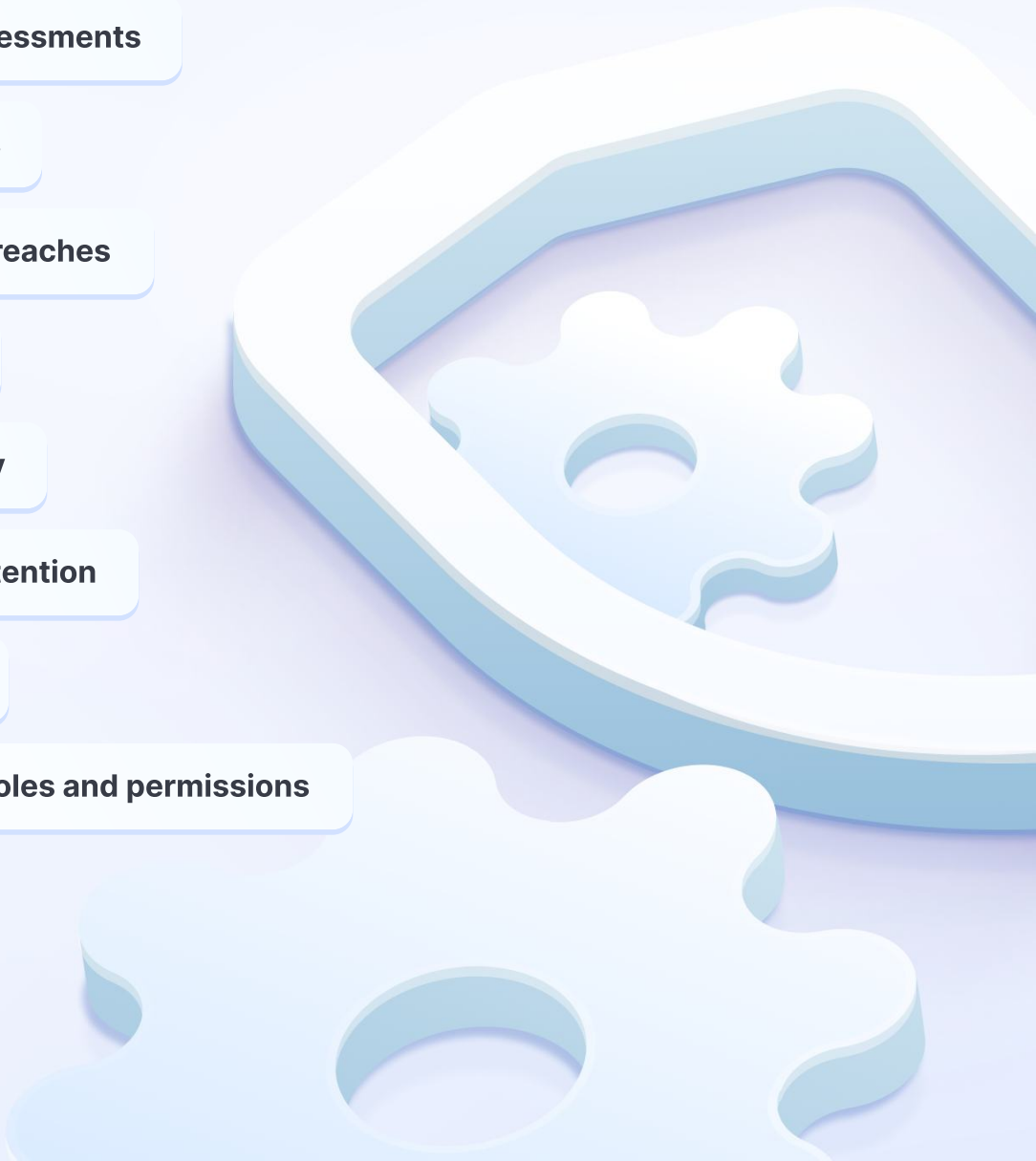
FundraiseUp

Nonprofit checklist for choosing secure software partners

Choosing the right software vendors and partners is critical for nonprofits, given their reliance on technology for mission-critical activities. However, assessing the security and reliability of software solutions can be daunting, especially with numerous vendors available.

This checklist will guide your nonprofit through the process of assessing potential software solutions, focusing on critical aspects of security, privacy, and compliance to safeguard your operations and data.

- [ ] **Compliance with regulations and standards**
- [ ] **Data privacy and protection**
- [ ] **Regular security assessments**
- [ ] **Anti-fraud measures**
- [ ] **Historical security breaches**
- [ ] **Incident response**
- [ ] **Backup and recovery**
- [ ] **Data deletion and retention**
- [ ] **Staff management**
- [ ] **Admin control over roles and permissions**



1. Compliance with regulations and standards

Why it matters

Nonprofit organizations are subject to various regulations and standards governing data protection and privacy.

Compliance is not only a legal requirement but also crucial to maintaining donor trust and safeguarding sensitive information.

What to check

Verify if the solution complies with:

- **ISO 27001:** Verifies that the management of information security is comprehensive
- **GDPR:** Regulates data protection and privacy in the European Union
- **PCI DSS:** Ensures secure credit card transactions
- **SOC 2**: Assures that data management practices are in line with industry standards
- **WCAG 2.1 AA:** Ensures web accessibility for all users, including those with disabilities

Things to note

While there are many certifications to consider, focus on those most critical to your organization's needs. For instance, although many providers may claim PCI DSS compliance, this alone does not guarantee comprehensive security.

Ensure the software itself, not just its data centers, is ISO certified and that these certifications are maintained with current assessments, not just historical ones.

2. Data privacy and protection

Why it matters

Safeguarding sensitive information is crucial for nonprofits to maintain the trust of donors and stakeholders. Effective data privacy measures ensure multi-layered security and the integrity of organizational data.

What to check

- **Privacy settings:**

  Confirm whether the solution has configurable privacy settings that adequately protect Personally Identifiable Information (PII)
- **Security features:**

  Determine if the solution includes comprehensive security features such as firewalls and encryption

Things to note

The vendor should provide a clear explanation of how data will be stored, transmitted, and protected. This detail is typically found in the Information Security Policy. Additionally, verify how the solution uses AI, ensuring that PII is not utilized in AI processes.

3. Regular security assessments

Why it matters

Regular security assessments are essential for identifying and mitigating potential vulnerabilities within a software solution.

What to check

- **Comprehensive testing:**
  Inquire whether the vendor has experienced any security breaches or significant security incidents in the past
- **Assessment frequency:**
  Ask about the steps taken to mitigate future risks following past incidents, including changes in policies, technologies, and processes
- **Third-Party evaluations:**
  Inquire whether risk assessments involve third parties who might have access to your data and how these evaluations are integrated into the overall security strategy

Things to note

Different types of audits may be conducted on different schedules. It is recommended that penetration testing be performed at least annually.

Ensure that the vendor provides ongoing evidence of their security assessments and doesn't rely on outdated certifications or past audits as proof of current security.

4. Anti-fraud measures

Why it matters

Implementing anti-fraud measures is critical for nonprofits to protect the donor experience and prevent financial losses due to fraudulent activities. Effective fraud prevention strategies help maintain the integrity of donation processes and enhance donor confidence.

What to check

Inquire whether the platform utilizes advanced anti-fraud tools.

Things to note

Anti-fraud measures should be an integral part of the platform's compliance and risk management framework.

5. Historical security breaches

Why it matters

Understanding a vendor's history with security incidents is crucial for assessing their reliability and their ability to respond to and recover from breaches.

What to check

- **Disclosure of past incidents:**
  Inquire whether the vendor has experienced any security breaches or significant security incidents in the past
- **Mitigation and response strategies:**
  Ask about the steps taken to mitigate future risks following past incidents, including changes in policies, technologies, and processes

Things to note

Maintaining the trust and confidence of donors, beneficiaries, and other stakeholders is essential.

Any security incidents or breaches can damage your organization's reputation and erode trust, leading to decreased support and funding.

6. Incident response

Why it matters

A comprehensive incident response plan is important for minimizing the impact of security breaches. It ensures that nonprofits can swiftly address security incidents, maintaining the integrity and trust of their operations.

What to check

- **Notification timeliness:**
  Verify how quickly the vendor commits to notifying your organization in the event of a breach or suspected security incident. The promptness of this notification is critical for effective mitigation
- **Data classification matrix:**
  Check if the Incident Response Policy includes a data classification matrix. This matrix helps prioritize security responses based on the sensitivity of the data involved

Things to note

The Incident Response Policy should outline the procedures for detecting, reporting, and responding to security incidents.

7. Backup and recovery

Why it matters

Reliable backup and recovery processes are crucial for ensuring data integrity and operational continuity in the event of data loss or system failures.

For nonprofits, this capability is essential to maintain trust and minimize disruption to their services.

What to check

- **Backup frequency and encryption:**
  Determine how frequently backups are performed and whether these backups are encrypted. This helps protect sensitive data even in backup storage
- **Mitigation and response strategies:**
  Check the duration for which backups are retained. A longer retention period can be beneficial for recovering older data if needed

Things to note

A Business Continuity and Disaster Recovery Plan usually clearly outlines the frequency and scope of backups as well as their retention times and encryption measures.

It's important to ensure that backups are performed at least daily and are retained for a sufficient period, typically at least a year, to meet both operational needs and compliance requirements. Also, verify that the solution provides mechanisms for secure and efficient data recovery.

8. Data deletion and retention

Why it matters

Proper management of data deletion and retention is crucial for nonprofits to remain compliant with data protection laws and to maintain donor trust. Ensuring that data is not retained longer than necessary, and that it can be securely deleted, protects against data breaches and misuse.

What to check

- **Data deletion procedures:**
  Verify the processes in place for securely deleting data from all systems, including backups, once it is no longer needed or upon request
- **Data retention policies:**
  Assess the vendor's data retention policies to ensure they align with legal requirements and organizational policies. Check how long different types of data are retained and the criteria used to determine these periods

Things to note

It's important for nonprofits to verify that the vendor's Data Protection and Handling Policy clearly outlines the methods used for data deletion.

9. Staff management

Why it matters	What to check	Things to note
Regular information security training and awareness programs are critical for preventing security breaches and ensuring that all staff are informed about the latest security practices and threats. This is particularly important for nonprofits, where sensitive donor information is often handled.	• **Background checks:** Ensure that the vendor performs comprehensive background checks on all employees, especially those who will have access to sensitive data • **Annual security training:** Verify that the vendor conducts annual security training for all employees. This training should cover current security practices, threat awareness, and how to respond to security incidents • **Role-Specific training:** Determine whether the vendor provides role-specific security training that addresses the unique needs and access privileges of different employee roles	It's crucial for the Information Security Policy to outline the vendor's overall approach to security training and awareness.

10. Admin control over roles and permissions

Why it matters	What to check	Things to note
Effective management of roles and permissions is crucial for maintaining security within a nonprofit's tech environment.	• **Flexibility of role assignments:** Determine if the solution allows administrators to assign and customize roles and permissions based on the specific needs and structure of your organization • **Ease of management:** Assess how easily roles and permissions can be managed within the platform (adding, modifying, or removing access as needed without requiring extensive technical support)	The ability for administrators to effectively manage roles and permissions directly impacts the security of sensitive data and the overall efficiency of your operations, while also helping to ensure compliance with various regulatory requirements.

How Fundraise Up secures nonprofit data

Download this Security Measures Guide for nonprofits for a deep dive into how Fundraise Up secures organization and donor data

Get the guide >