Political Tech Vendor Best Practices

This document aims to provide a checklist of best practices that all vendors of technology for the campaign industry should deliver. The recommendations should be achievable, even for a venture-backed company with limited staff and resources.

The goal is to standardize requirements so National Committees, State Parties, IE Customers and Campaigns can write them into RFPs and contracts and so vendors can anticipate them in product design and delivery.

We recognize practical reality means some recommendations may need to be adjusted or phased in over time. In all cases, however, we **opted to make the best possible recommendation** to provide an aspirational target to work toward.

Service Level Agreement

All contracts should include language which requires the following of any vendor providing software or technology services for the campaign ecosystem:

- ❏ Guarantee at least 99% uptime/availability for all major features, including access to view and download data. Uptime should be calculated monthly.
- ❏ Define both Standard and Extended Business Hours, during which specified levels of support and responsiveness can be required.
    - ❏ For example, Standard Business Hours could be defined as 9AM to 9PM Eastern Time (excluding weekends) and Extended Business Hours could be defined as 9 AM to Midnight Eastern Time (including weekends).
    - ❏ During a specified period of time prior to the general election (e.g., 2 months), Extended Business Hours should become Standard Business Hours to account for increased activity as the election nears.
- ❏ Scheduled downtime should be allowed outside of Extended Business Hours with at least 7 days notice, and during Extended Business Hours with 10 days notice.
    - ❏ Key customers (e.g., Committees and State Parties) should have a mechanism to consider and reject a planned outage if it is going to occur during a specified period of time prior to the general election (e.g., 2 months).
    - ❏ Companies should not perform updates for anything other than crucial stability and bug fixes from 3 months before the general election until two weeks after election day without the permission of key customers.
    - ❏ Companies must maintain the ability to roll back any update within 60 minutes, should an update create an outage or serious disruption of the service.
- ❏ Define what constitutes an outage, support tiers and issue severity. Define Support and Responsiveness requirements for each tier and severity and include an escalation path. For example:
    - ❏ Respond to all Outages and Showstopper issues and notify customers within 1 hour.

- ❏ Respond to High severity issues within at least 4 hours during Extended Business Hours.

Security

All contracts should include language which requires the following security features of any vendor providing software or technology services for the campaign ecosystem:

- ❏ Products must provide account sign-on using a consumer third-party identity service that supports the ability to configure specified accounts for Security Key-only 2FA.
  - ❏ Currently the only recommended identity service provider is Google.
  - ❏ **Note:** Microsoft has announced plans to support Security Key 2FA through its Microsoft Hello service, so in future they may be a valid provider as well.
- ❏ Products must have a role-based permission structure that allows creation of at least:
  - ❏ Sensitive roles (access to sensitive data and services) which require Security-Key only 2FA.
  - ❏ Staff/volunteer roles (cannot access key data and services) which do not require Security Key-only 2FA.
- ❏ Products must encrypt all data that is on its servers, stored on the device/client, and when the data is being passed between server and client.
- ❏ Product must be hosted and operated on a top-tier cloud platform.
  - ❏ Specifically, top-tier should be defined as one of Amazon Web Services, Google Cloud Platform, or Microsoft Azure.
  - ❏ All cloud hosted resources must reside within the United States to avoid being subject to the data sovereignty and reporting laws of foreign countries.

Business Practices

The following baseline business practices should be written into contracts with any vendor providing software or technology services for the campaign ecosystem:

- ❏ Data Ownership
  - ❏ The customer retains all rights to data generated by their activity using the software or service. They may require, via written request, that the vendor delete all of their data at any time during or after provision of services.
  - ❏ Vendors retain the right to generate and use aggregate data (data which is not tied to a single customer or individual) for business purposes during or after the term of the agreement. Examples of valid usage would be: execution of services, developing and improving products and services, identifying and publicizing best practices).
  - ❏ Vendors may not use, copy, sell, or otherwise access non-aggregate customer data before, during or after the provision of services to the customer, without written consent.
- ❏ Publicity - the vendor cannot discuss or disclose any information about the customer or their work before, during or after the provision of services to the customer, without written consent.
- ❏ Rights of Termination
  - ❏ The customer must be able to terminate the agreement for any reason with reasonable notice (e.g., 30 days).

- ❏ The vendor cannot terminate the agreement, without justification, until 2 weeks after key events which should be defined in the contract (such as the general election).

❏ Vendor Security

- ❏ Vendor must require key-based 2FA on all accounts used to communicate with or transfer data to/from customers.
- ❏ Contracts should outline the required response in the event that a Vendor suffers any type of Security or Data breach. For example:
  - ❏ Notify customers in a reasonable amount of time (which should be defined in the contract).
  - ❏ Provide a single point of contact who is available 24x7 to assist Customer with investigating and remedying the issue.
  - ❏ Not provide any public disclosure or statement without written consent, unless required by law.

Have questions or comments?

Let us know at info@digidems.com