Selecting a Digital Services Vendor
Checklist

This checklist is a supplement to the [Choosing A Vendor for Digital Services](#) handout and is not meant to be a stand-alone tool. Before using this tool, please read through the main document, which describes key concepts and dives deeper into each section included in this tool.

Please also see the entire [Digital Services Toolkit](#) for additional information about [Assessing Readiness for Digital Services](#) and [Best Practices for Digital Services](#). [Safety Net is also available](#) to provide technical assistance, including assisting in evaluating the suitability of specific platforms for your program's needs.

Vendor: _____

Contact Name: _____ Contact Email / Phone: _____

Platform Related Costs

ITEM	COST	ONE-TIME OR ONGOING?	YEARLY ESTIMATE
Purchase & Setup	$	❑ one-time ❑ ongoing	$
Use Fees	$	❑ one-time ❑ ongoing	$
Maintenance	$	❑ one-time ❑ ongoing	$
Other:			

Data Security & Privacy

Does the platform keep a record about each conversation? (e.g., date, time, IP address, phone number, etc.)	❑ **Best:** No identifying data is recorded. ❑ **OK:** Data is deleted automatically and quickly (within 1-3 days). ❑ **Caution:** Data can be deleted, but less often or only manually. ❑ **Unacceptable:** Data is kept indefinitely. ❑ **Not clear:** (Ask vendor.)
Does the platform store transcripts of the conversation?	❑ **Best:** Content automatically disappears after a conversation ends. The vendor cannot access the content at any point. ❑ **Caution:** Content can be deleted, but is kept for a time or must be manually deleted. ❑ **Unacceptable:** Content is kept indefinitely. ❑ **Not clear:** (Ask vendor.)
Is any conversational related content included in the automatic backup process? (e.g., transcript, IP addresses, etc.)	❑ **Best:** There is no automatic backup process. ❑ **OK:** There is an automatic backup process, but you can turn it off and/or set up automatic deletion. ❑ **Caution:** There is an automatic backup process, and you have to manually delete the backup data. ❑ **Unacceptable:** There is automatic backup process, and you can't delete the backup data. ❑ **Not clear:** (Ask vendor.)
Is data encrypted in transit? At rest?	❑ **Best:** Data is encrypted in transit and at rest. ❑ **Caution:** Data is encrypted only in transit.

	❑ **Unacceptable:** Data is not encrypted. ❑ **Not clear:** (Ask vendor.)
Can the vendor see personally identifying victim information?	❑ **Best:** It is not technologically possible for anyone in the vendor's company to see or access personally identifying victim information (Including phone numbers, IP addresses, content of conversations). The vendor doesn't hold a copy of the encryption key. ❑ **Caution:** The program has a contract in place with the vendor specifying policies and penalties to prevent vendor employees from accessing conversations or data about conversations. ❑ **Unacceptable:** Vendor employees can access conversations or data about conversations, and no policies or penalties are in place. ❑ **Not clear:** (Ask vendor.)
Do they use hardware or services of a third-party company separate from their own?	❑ **OK:** Third party companies' access to data do not reveal personally identifying information of survivors who contacted the program. ❑ **Caution:** Third party companies have access to personally identifying data, but an agreement is in place specifying policies and penalties to protect against employee access to conversations or data about conversations. ❑ **Unacceptable:** Third party companies' employees can access conversations or data about conversations, and no policies or penalties are in place. ❑ **Not clear:** (Ask vendor.)

Will they share or release personally identifying victim data? If yes, under what circumstances? How do they respond to requests from government, law enforcement, lawyers?	❑ **Best:** The vendor will fight any legal request, using their own resources. They will also notify you <u>before</u> they comply, so you can also fight the request. Additionally, all data is encrypted and the vendor doesn't have access to unencrypted data, so they cannot release or share any unencrypted data anyhow. ❑ **OK:** They will notify you of a request, so you can fight the request. ❑ **Caution:** The vendor will notify you of a legal request, but will comply with the request. ❑ **Unacceptable:** The vendor will release or share the data without notifying you of the request. ❑ **Not clear:** (Ask vendor.)
Will they provide notice of a data breach?	❑ **Best:** They will notify you immediately and assist with remedies. ❑ **OK:** They will notify you immediately. ❑ **Caution:** They will notify you, but the timeline is unclear. ❑ **Unacceptable:** They will not notify you of a data breach. ❑ **Not clear:** (Ask vendor.)

Features & Customizability

Does the platform support emojis, pictures, and video? Can that be turned off?	❑ **OK:** The platform allows emojis, pictures, and/or videos, and you can customize the settings to turn off some or all. ❑ **Caution:** The platform allows emojis, pictures, and/or videos, but you cannot turn them on or off to create a default for whether they are available for use. (This means you'll have to rely on telling

	advocates and survivors whether or not they should use these features.) ❑ **Not clear:** (Ask vendor.)
Do they offer language translation? Is it provided by a machine or a person?	❑ **Best:** The platform allows for a skilled live interpreter to join the conversation. ❑ **Caution:** The platform offers machine translation that can be turned off. ❑ **Unacceptable:** The platform offers machine translation that can't be turned off. ❑ **Not clear:** (Ask vendor.)
Can you set up "canned" or cut-and-paste messages?	❑ **Best:** The platform allows you to write an unlimited number of canned messages that can be easily inserted into a conversation and can be updated any time. ❑ **OK:** The platform allows a limited number of canned messages, and you have to ask the vendor to make updates or changes to the messages. ❑ **Caution:** The platform only offers standard messages that you can't edit, and which don't suit your program. ❑ **Not clear:** (Ask vendor.)
Are there indicators that someone is typing? (e.g., "Matt is typing…")	❑ **OK:** If the platform includes this feature, you have the option to turn it off. ❑ **Caution:** The platform includes this feature, and you can't turn it off. ❑ **Not clear:** (Ask vendor.)

Is there cross-platform integration? (e.g., can a survivor reach out through text, social media, and secure chat, etc.)	❑ **OK:** The platform doesn't offer this. Or, the platform does offer this, but you can turn the feature on or off by platform (for example, some cross-platform integration may not be preferable). ❑ **Unacceptable:** The platform offers these integrations, and you can't turn it on or off. Some identifying data might be shared across platforms. ❑ **Not clear:** (Ask vendor.)
Do survivors need to download an app in order to use the platform?	❑ **Best:** The survivor doesn't need to download anything. ❑ **Caution:** Survivor would need to download software or an app. *(This may only be acceptable for survivors whom the agency has been able to assess risk and safety plan, including downloading the app).* ❑ **Unacceptable:** Survivor would need to download software or an app. *(This could be a safety risk for survivors in crisis or who have not had a chance to assess their risk or safety plan around the use of tech.)* ❑ **Not clear:** (Ask vendor.)
Do survivors need to create a user account, profile, or screen name?	❑ **Best:** The platform doesn't require an account, profile, or user name. ❑ **OK:** The survivor needs to create an account, profile, or user name, but no identifying information is required to create the account. *(Only OK for platforms used for ongoing clients only – not crisis lines.)* ❑ **Unacceptable:** A survivor would need to set up an account, profile, or user name. *(For platforms being used for crisis response lines.)* ❑ **Not clear:** (Ask vendor.)

Can you access personally identifying data about survivors at any time? Can you delete it at any time?	❑ **Best:** Personally identifying data is not stored. ❑ **OK:** Personally identifying data is automatically deleted promptly and regularly, and/or you have complete control over, and access to, any personally identifying data. ❑ **Caution:** You need the vendor's assistance to access or delete personally identifying data. ❑ **Unacceptable:** You can't access or delete data that is personally identifying. ❑ **Not clear:** (Ask vendor.)
Can you assign different access levels to users (advocates, managers, etc.)?	❑ **Best:** You have full control over access levels, can add or delete users, and change their access levels at any point without vendor assistance. ❑ **OK:** You have to request that the vendor add and delete users and change their access levels. The vendor will immediately process the changes. ❑ **Caution:** You have to request changes from the vendor, and the changes are not processed immediately. ❑ **Unacceptable:** All users have the same access level, which includes access to personally identifying victim data. ❑ **Not clear:** (Ask vendor.)

Customer Service

Technical support & troubleshooting	❑ **Best:** The vendor offers 24/7 dedicated technical support and customer service.
	❑ **OK:** The vendor does not have 24/7 technical support, however they respond to questions in a reasonable amount of time. The platform is easy enough to use, and your staff and volunteers can likely resolve common problems OR you have dedicated IT staff or consultants who can help.
	❑ **Caution:** The vendor doesn't have a dependable technical support or customer service team. Your agency has dedicated IT staff who are comfortable with the platform and have sufficient access to help.
	❑ **Unacceptable:** The vendor doesn't have dependable technical support and your agency does not have access to IT staff.
	❑ **Not clear:** (Ask vendor.)
Is there any limit on the number of users from your program?	❑ **Best:** There are unlimited users (including for your staff and people who reach out to you for help).
	❑ **OK:** Limits on users (for your staff and people who are seeking help) are well above your anticipated need, and cost for additional users is reasonable.
	❑ **Caution:** Limits on users (for your staff and people who are seeking help) are just enough. Cost for additional users is significant.
	❑ **Not clear:** (Ask vendor.)

What Internet bandwidth is required to use the platform?	❑ **Best:** Your program won't need to upgrade Internet bandwidth or equipment.
	❑ **OK:** Your program has the budget to make any necessary upgrades.
	❑ **Caution:** The vendor isn't sure if you'll need upgrades.
	❑ **Unacceptable:** The required bandwidth isn't available in your area, and/or you can't afford to make upgrades.
	❑ **Not clear:** (Ask vendor.)
What is their record regarding system downtime? What are their plans in case of unexpected downtime? Will their regular maintenance impact your services?	❑ **Best:** The vendor has systems in place to avoid scheduled downtime, and a plan for unexpected downtime.
	❑ **OK:** The vendor gives advance notice of scheduled downtime and works to ensure it will have minimal impact on users. They also have a plan for unexpected downtime.
	❑ **Caution:** The vendor has scheduled downtime that interferes with your services, and/or they have no plan for unexpected downtime.
	❑ **Not clear:** (Ask vendor.)

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.