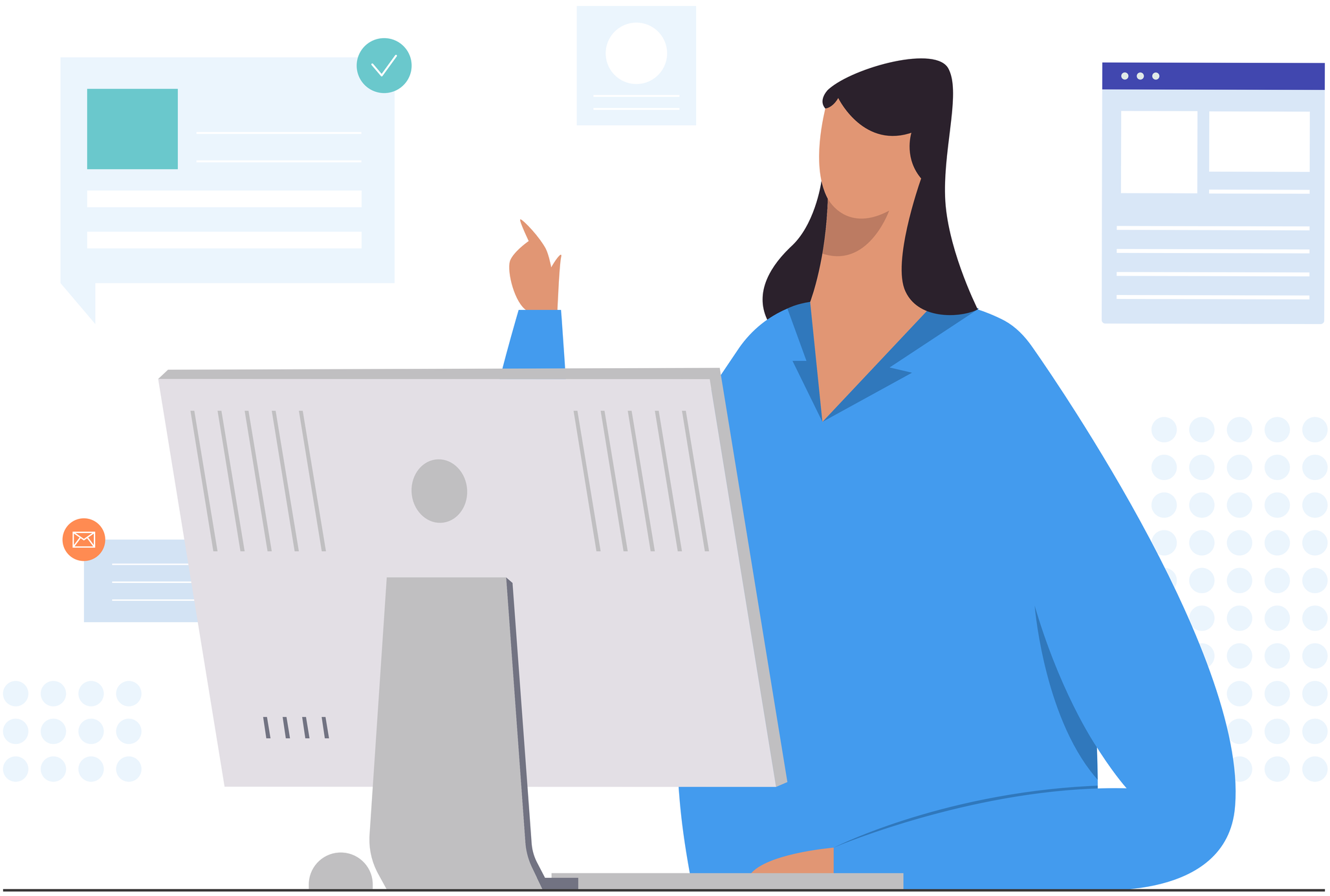
Ivy.ai

Example AI **Chatbot Requirements**

A Guide For Developing AI Chatbot Requirements for Higher Education



Features

As is the case with any SaaS solution, it's imperative to source a solution that provides features that support your goals. Institutions seeking to improve user outcomes while simultaneously easing staff burden must source a solution that maximizes efficiency, configurability, and accessibility. The following example requirements will help to identify a state-of-the-art solution that can be customized to support your needs.

Feature Requirements:

- The solution must include an automated 24/7 AI chatbot across multiple communication channels with fewer than 10% of interactions resulting in search results, a response of "I do not know," or other similar indirect responses.
- The solution must be custom-built to understand topics unique to each department or campus, rather than taking a one-size-fits-all approach via templated content.
- The solution's AI chatbot must reside on the institution's website by default, rather than an external platform or app.
- The solution's AI chatbot must be accessible to users on channels other than the institution's website, such as social media platforms, SMS text, mobile applications, et al.
- The solution must integrate with "at home" devices, such as Amazon Alexa, to allow users to interact with the bot.
- The solution must provide administrators with tools to edit or add responses as needed without assistance from the vendor.
- The solution must support the institution's entire enterprise. Individual chatbots in various departments must be able to share content, providing seamless access to information across multiple departments and platforms.
- The solution must monitor the institution's website for updated information and alert administrators to discrepancies between web content and chatbot knowledge, or adjust chatbot responses accordingly.
- The solution must provide administrators with tools to edit and update existing chatbot knowledge individually and in bulk.
- The solution must provide a mechanism for automatically detecting and obfuscating, masking, hiding, or otherwise protecting Personally Identifiable Information entered by end users.
- The solution's AI chatbot must get more intelligent with time by receiving input from administrative users who wish to add chatbot knowledge, and by retraining the AI algorithm on a regular interval to improve the chatbot's ability to understand natural language questions.

- The solution must be accessible from any device and must not require installation of a mobile app.

- The solution must understand and continue conversations that use typos and/or slang.

- The solution must understand questions that include institutionally-unique pronouns, such as “Where is the Smith Center located?”

- The solution’s chatbot must incorporate sentiment analysis to detect user emotions and offer a conversational feel.

- The solution must provide administrators with the ability to customize the chatbot’s name, interface colors, etc., to align with the institution’s branding.

- The solution must automatically communicate with users in at least 100 languages without the need to create and manage knowledge in each language.

- The solution must provide unlimited accounts for live agents to provide chat support over web and SMS. And, If no live agents are available, the system must route the user’s question to a designated inbox so that it can be answered directly.

- The solution must offer AI guidance and suggested messaging to live agents during live chat interactions.

- The solution must provide the ability to configure decision trees and complex messaging sequences to guide students through processes, such as applying for financial aid.

- The solution must allow staff to configure text message campaigns to be sent on an ad-hoc basis or scheduled to run on specific dates.

- The solution must provide the ability to personalize text messages being sent in a campaign to include data points such as student name or a missing item needed to complete various institutional tasks.

- The solution must provide the ability to run surveys via text message campaigns and report on the results.

- The solution vendor must provide a robust support package, including a dedicated support team, product guides, training videos, and opportunities for ongoing live training.

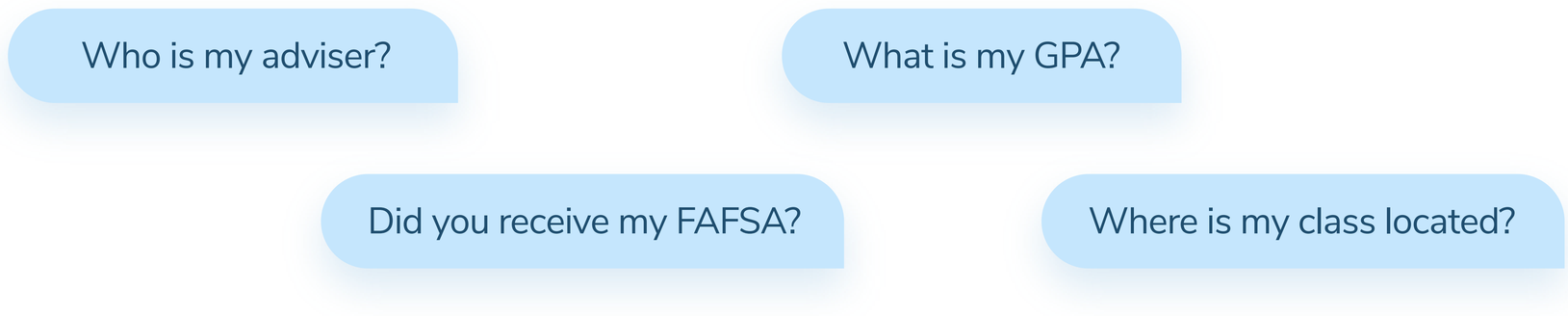
- The solution vendor must provide technical and diagnostic support via phone, email, and helpdesk ticketing.

Integrations

Integrations are the vehicles that connect your chatbot's knowledge to your other systems. This makes it possible to provide a personalized, 1:1 experience for end users, as well as enhance the overall user experience. Additionally, integrations make it possible to streamline the flow of data from your end users to third-party systems. The following example requirements will help to identify a solution with the necessary integration capabilities to facilitate this objective.

Integration Requirements

- The solution's chatbot must be able to automatically request basic contact information for additional follow-up and lead generation when accessed from the institution's website.
- The solution must automatically send lead information collected on the website as part of the chat function to the institution's desired CRM.
- The solution must integrate with the institution's CRM using a real-time API integration. The vendor must develop and/or configure the integration. At a minimum, the integration should support writing the full chat or text transcript back to the student's record in the CRM.
- The solution must integrate with enterprise platforms using a real-time API integration. The vendor must develop and/or configure the integration. The integration should support the chatbot's ability to answer questions such as the following after the end-user has authenticated:



- The solution's chatbot must be able to connect to email inboxes and auto-respond to inbound emails.
- The solution must integrate with Google Analytics and Google Tag Manager, with Tags that represent end user engagement out-of-the-box.
- The vendor should indicate authentication methods (SAML, Shibboleth, Active Directory, etc.).

Reporting and Analytics

In order to understand and measure the ROI of any solution, administrators must have the ability to generate reports and analyze data. Institutions should seek a solution that provides a window of visibility into performance for the technology and the people who support it, as well as the overall ability of the technology to meet and exceed end user expectations. The following example requirements will help to identify a solution that provides such visibility.

Reporting and Analytics Requirements

- The solution must provide the ability to report on the types and numbers of questions being asked, most-asked about topics, times throughout the year where certain questions are trending, and other such insights. The system shall have the ability to show this information by communication channel such as via the website or text message.

- The solution must provide administrators with the ability to view questions to which the chatbot did not know the answer. Furthermore, administrators must be able to easily add knowledge to improve the chatbot's ability to answer such questions in the future.

- The solution must provide administrators with the ability to view the chatbot's overall accuracy when delivering timely, relevant responses to end users.

- The solution must offer end users the ability to rate their experience with the chatbot, and that rating information should be viewable by an administrator in a report or dashboard.

- The solution must provide administrators with the ability to export and download all measurable data on demand.

- The solution must provide a dashboard of standard, out-of-the-box reports that deliver insights into chatbot performance, live agent performance, and user satisfaction.

- The solution must provide standards reports that, by default, can be configured by administrators to reflect custom time periods.

- The solution must gather and store transcripts for all chat conversations, availing them to authorized administrators and end users on demand.

- The solution must provide report detail on conversion rates of end users that were part of text message campaigns to understand engagement and campaign effectiveness.

Technical Specifications

To provide a seamless experience for all end users, institutions need to source a solution that is compatible with a variety of other technologies. An ideal solution should support all of the following example technical specifications.

Technical Specifications

- The solution must support single sign-on for both the chatbot interface and any administrative portal.
- The solution must support end-users accessing the bot interface using multiple web browsers and devices.
- The solution must allow administrative users to access the administrative portal from mobile devices.
- The solution must incorporate role-based access for users.
- The vendor must describe their password policy including password strength, password generation procedures, password storage specifications, and frequency of password changes.
- The solution must permit the use of multi factor authentication for administrators.
- The vendor must indicate the administrative safeguards and best practices they have in place to vet their employees.
- The vendor must indicate whether they employ third party contractors and what administrative safeguards and best practices they have in place to vet third-parties' staff members.
- The vendor must detail the procedures and best practices in place to ensure that user credentials are updated and terminated as required by changes in role and employment status.
- The vendor must have a strategy in place for platform upgrades and patches for both the server and software. The vendor should provide a release schedule, recommended processes, estimated outage durations, and plans for upcoming major upgrades.

Accessibility

Accessibility within your website is essential for your institution to create a high-quality user experience. By addressing and prioritizing robust accessibility features in your request for proposal, your institution displays your commitment to inclusivity and equal opportunity.

- The solution must provide a chatbot interface that is accessible and compliant with Web Content Accessibility Guidelines (WCAG) version 2.0, levels A and AA.
- The vendor must submit an Accessibility Conformance Report (ACR) for their solution, which must be based on a Voluntary Product Accessibility Template® (VPAT®), version 2.1 or higher.
- The vendor must provide a supplemental accessibility statement including the vendor's commitment to providing accessible solutions.
- The solution must address the following:
    - Any accessibility or usability features provided by the solution.
    - Any known accessibility limitations of the solution.
    - Any configuration or installation requirements to provide accessibility.
    - Ability to operate the application using only the keyboard, including a visual focus indicator and logical navigation order.
    - Ability to operate the application with a screen reader (i.e., JAWS, NVDA, VoiceOver).
    - Ability to zoom the text size without loss of functionality.
    - Description of the solution's color contrast ratio for text and images of text.
    - Description of where users can find accessibility features, settings, and support within the application.

Security Specifications & Data Protection

A solution that meets or exceeds your institution's security requirements is critical. With the transmission of personally identifiable information, data protection is an essential feature that must be prioritized when selecting a vendor.

- The solution must be tested for application security vulnerabilities, such as an evaluation against the Open Web Application Security Project (OWASP) Top 10 list that includes flaws like cross site scripting and SQL injection. Results should be provided.
- The vendor must specify how they will implement critical security updates.
- The vendor must indicate whether they will permit the institution to conduct a penetration test on the institution's instance of the chat solution.
- The solution must utilize a secure, encrypted method of transport for confidential, sensitive, or otherwise protected data transmission.
- The vendor must describe the physical access controls used to limit access to the data center and network components.
- The vendor must describe the procedures and best practices in place to harden all systems that hold, process, or have access to sensitive data.
- The vendor must describe technical security measures in place to detect and prevent unintentional, accidental and intentional corruption or loss of records.
- The vendor must describe procedures it has in place to detect information security breaches and notify customers.
- The vendor must describe procedures to isolate or disable all systems in the event a security breach is identified.
- The vendor must describe the safeguards in place to prevent the unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access, or disclosure of the institutions records.
- The vendor must have a data backup and recovery plan supported by policies and procedures. Briefly describe the plan, including scope and frequency of backups, and how often the plan is updated.
- The vendor must describe the methods used to encrypt backup data or alternative safeguards in place to protect backups against unauthorized access.
- The vendor must provide information on data retention timelines and procedures in place for disposing of records.

Regulatory Requirements

The following sample requirements are essential to maintaining your institution's compliance with state and federal regulations.

- The vendor must describe the procedures and methodology it has in place to retain, preserve, backup, delete, and search data in a manner that meets the requirements of U.S. federal and state electronic discovery rules, including how and in what format records are kept and what tools are available to the institution to access records.

- The vendor must describe its processes for ensuring that data is protected in compliance with all applicable U.S. federal and state requirements, including export control.

- The solution must comply with all applicable laws and regulations commonly found in a higher education environment as well as the timely implementation of compliance with future changes to laws and regulations. Current laws and regulations include, but are not limited to FERPA, HIPAA, the Clery Act, etc.

- The vendor must list and describe any regulatory or legal actions taken against vendor for security or privacy violations or security breaches or incidents, including the final outcome.