



STAFF ALERT DEVICE BUYER'S GUIDE

Version 1.0

April 2, 2019

About HTNG

Hospitality Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hospitality community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitates the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

Copyright 2019, Hospitality Technology Next Generation

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

For any software code contained within this specification, permission is hereby granted, free-of-charge, to any person obtaining a copy of this specification (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the above copyright notice and this permission notice being included in all copies or substantial portions of the Software.

Manufacturers and software providers shall not claim compliance with portions of the requirements of any HTNG specification or standard, and shall not use the HTNG name or the name of the specification or standard in any statements about their respective product(s) unless the product(s) is (are) certified as compliant to the specification or standard.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES, OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF, OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Permission is granted for implementers to use the names, labels, etc. contained within the specification. The intent of publication of the specification is to encourage implementations of the specification.

This specification has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed. Visit <http://htng.org/ip-claims> to view third-party claims that have been disclosed to HTNG. HTNG offers no opinion as to whether claims listed on this site may apply to portions of this specification.

The names Hospitality Technology Next Generation and HTNG, and logos depicting these names, are trademarks of Hospitality Technology Next Generation. Permission is granted for implementers to use the aforementioned names in technical documentation for the purpose of acknowledging the copyright and including the notice required above. All other use of the aforementioned names and logos requires the permission of Hospitality Technology Next Generation, either in written form or as explicitly permitted for the organization's members through the current terms and conditions of membership.

TABLE OF CONTENTS

1	DOCUMENT INFORMATION	4
1.1	DOCUMENT PURPOSE.....	4
1.2	RELATIONSHIP TO OTHER STANDARDS	4
1.3	OVERVIEW	4
1.4	FURTHER CONSIDERATIONS	5
2	COMPANY BACKGROUND	6
3	PRODUCT INFORMATION	8
4	ADDITIONAL PRODUCT INFORMATION	14
5	DEPLOYMENT & INSTALLATION	16
6	TRAINING	18
7	TECHNICAL QUESTIONS	20
8	ACCOUNT MANAGEMENT & SUPPORT	24
9	INTEGRATION	26
10	UPGRADES	27
11	SCALABILITY	28
12	PRICING	29
13	CONCLUSION	30
14	APPENDICES	31
14.1	GLOSSARY OF TERMS.....	31



1 DOCUMENT INFORMATION

1.1 DOCUMENT PURPOSE

The hospitality lodging industry has always been driven by the purpose of providing the optimal guest experience and care. Hotel brands have long recognized the importance of providing a safe and supportive environment for their employees to empower them. Recently, many hotel brands have promised to provide staff alert devices to their employees to urgently and easily request assistance to their location.

There are potentially thousands of hotels that may need to select and deploy solutions to meet unique requirements and diverse environments. Members of the trade association, Hospitality Technology Next Generation (HTNG), have developed this buyer's guide to assist hoteliers, from general or operations management to corporate brand executives, build a Request for Information (RFI) or Request for Proposal (RFP) for their brands. The objective of this guide is to assist the procurement team to identify the most relevant questions, and to allow the development of the tailored RFI or RFP for their property or brand.

1.2 RELATIONSHIP TO OTHER STANDARDS

The American Hotel & Lodging Association (AHLA) and the major hotel brands announced the 5-star promise in September 2018. This promise was “a pledge to provide hotel employees across the U.S. with employee safety devices (ESDs) and commit to enhanced policies, trainings and resources that together are aimed at enhancing hotel safety, including preventing and responding to sexual harassment and assault.”¹

Similar to HTNG's Staff Alert Technology Workgroup, AHLA has a task force of industry participants to begin the process of outlining an implementation framework. HTNG and AHLA are committed to working together to back the 5-star promise and deliver positive results to the hospitality industry.

1.3 OVERVIEW

This document is divided into thirteen sections. Each section contains a title, overview, sample questions to include in an RFI or RFP and additional context to guide response expectations.

Follow these steps to maximize the potential of this document:

- Review the questions and additional context
- Identify the questions that are most relevant to the needs of your property or properties and your brand(s)
- Consider your wireless infrastructure and technology requirements, limitations and any planned upgrades
- Evaluate any other unique needs

¹ American Hotel & Lodging Association (AHLA). (2018). Hotel industry announces added safety measures for employees; builds on layers of security procedures [Press release]. Retrieved from https://www.ahla.com/sites/default/files/5Star_PR_Brand.pdf

Please Note: The use of the term “Buyer” in this document refers to the RFP Issuing Party. It is important for a vendor who is responding to an RFI/RFP to understand your property and your unique requirements. Therefore, it would be helpful to include the following background information about your hotel and/or properties:

- Number of properties
- Locations of properties
- The number of employees you intend to provide an alert device to
- The hours of the security team
- What areas need to be covered (e.g. guest rooms, public spaces, etc.)
- Description of your IT Infrastructure
- Description of your operations and operations limitations, for example:
 - Do you have a security team, and if not, who responds to emergencies?
 - Hours of the security team, if you have one
- Description of your layout (e.g. a campus vs a high-rise)

1.4 FURTHER CONSIDERATIONS

Organizations should make sure they are fully educated on any local, state or government regulations and laws that they may legally need to oblige by. Some questions in this Buyer's Guide may be more important than others due to potential geographical obligations.



2 COMPANY BACKGROUND

The company's solutions, size and history will give greater insight into whether this organization is the right fit for your properties/brand and whether this organization can deliver on their promises.

	Sample Questions from Buyer to Provider	Question Context and Response Expectations
2.1	<ul style="list-style-type: none"> Where are you incorporated? Where is your head-office and any relevant regional office located? What is your Corporate Registration Number? 	Head Office address and corporation number – could be FEIN (Federal Employment Identification Number, also known as a Tax ID), DUNS (Dun & Bradstreet Number) or equivalent depending on the location of the headquarters. If there is a regional office (i.e. Europe, Middle-East etc.) this should also be provided.
2.2	Describe your company or division that is providing hospitality solutions. Include: <ul style="list-style-type: none"> Information about executive managers Relevant experience in hospitality Organizational structure 	A short narrative about each individual and their experience in hospitality or any associated industries. Highlighted experience in the industry should include years in the industry, employer name(s) and job titles.
2.3	<ul style="list-style-type: none"> Are you WBE, MBE, SDB, a Veteran Certified company or a certified Equal Opportunities Employer? How many of your suppliers/vendors are WBE, MBE, SDB or Veteran Certified Companies? If applicable, please provide certificates and data of issuance and expiration of the certificate(s).	This will vary depending on the region. Each of the accreditations will have some form of certification which the vendor is encouraged to include in their response. For reference: <ul style="list-style-type: none"> WBE – Women Business Enterprise MBE – Minority Business Enterprise SDB – Small Disadvantaged Business Veteran – Veteran Owned Business
2.4	Other than those mentioned above, what other certifications does your company have? Note: Please list any technical certifications in the technology section, specifically question number 7.5.	
2.5	Provide the total number of properties, property sizes and total number of devices that you have installed your solution across each unique industry (e.g. hotels, hospitals,	This question gives insight into: <ol style="list-style-type: none"> A scale of business solutions How focused the business is on hospitality



	campus), geographic regions (e.g. country, multi-state region, provinces, municipalities).	<ol style="list-style-type: none"> 3. What experience the vendor may have in adjacent industries 4. The degree of geographic presence
2.6	What other industries do you focus on other than hospitality for staff alert technology?	This is for information only and will support the information previously advised – however, it may also show that the vendor has a greater focus on other industries.
2.7	<p>Provide at least 3 references of properties of similar size and in our geographic region using the alert devices solution.</p> <p>This information should include:</p> <ol style="list-style-type: none"> 1. Property name 2. Contact name and title 3. Contact phone and email 4. Property size 5. Number of devices 6. Date of install 7. Property location(s) 	Buyer should indicate the size of the properties they wish to be included in this comparison.
2.8	<p>Optional Background Information:</p> <p>Where available, provide audited financial statements for the past two years and the amount of revenue related to this product or solution.</p>	<p>Buyer should reference supporting financial information as part of an appendix. The vendor may be asked to provide audited statements, if available.</p> <p>The vendor may request the client to confirm complete confidentiality of the financial information provided.</p>

3 PRODUCT INFORMATION

This section includes questions useful for assessing the product protocols, capabilities and accuracy of the solution. This is the foundation to evaluate whether the solution will meet your unique needs and expectations.

	Sample Questions from Buyer to Provider	Question Context and Response Expectations
3.1	<p>Describe the technology your product uses to determine the location of the individual who activates the staff alert device.</p> <p>Include an operating diagram of your solution.</p>	<p>This question helps the vendor detail the solution's technology.</p> <p>Selection of a solution for your property may be dependent on the hotel's current building and technology infrastructure and renovation plans. Some of these methods may include GPS, Bluetooth beacons, Wi-Fi mapping or another location-based technology used to pinpoint an alert device.</p> <p>For example, if the hotel has or is updating its rooms with door locks, environmental controls, and guest Wi-Fi, the opportunity to leverage different technologies may exist.</p>
3.2	<p>Does your solution provide updated location of the employee (i.e. "follow-me" feature) if the staff moves after the staff alert device has been activated?</p>	<p>This is the ability of the alert device solution to provide an updated or latest location of the employee in case they move or are moved after activating the alert device. It is important to know the ongoing location of the employee which could help responders decrease their response times.</p> <p>Some local ordinances or union contracts may require the solution to include this feature.</p>
3.3	<ul style="list-style-type: none"> • Does your solution identify its ongoing location when activated? • If so, how often does the staff's device transmit its location after being activated? • What is the typical, best and worst reporting times given the environment? 	<p>Some solutions may identify and report the location of the alert device after activation in one of the following ways:</p> <ul style="list-style-type: none"> • Only once • At set time intervals <p>Each type of location solution will have different costs, levels of accuracy dependent upon the environment of the building, network transport and service-level expectations.</p>
3.4	<p>Describe the technology your product uses for communication from the activated device</p>	<p>The technology used to locate staff (referenced in 3.1) may be the same or</p>



	<p>to the receiving system, and from the receiving system to the designated responder(s)? (e.g. BLE, RF, Ultrasonic, Wi-Fi, cellular, multiple technologies, etc.)</p>	<p>different than the technology used to communicate the location. It is important to know all technologies leveraged by the solution.</p> <p>The vendor should provide an overview of the different technology means it uses to communicate.</p> <p>Consider the current network infrastructure and reliability at the property. If the solution is dependent upon shared wireless spectrums such as cellular/LTE/CBRS or Wi-Fi, a site survey of the wireless network coverage of all areas should be considered with any proposal.</p>
3.5	<p>How does your staff alert device work? Please describe the following:</p> <ul style="list-style-type: none"> • How is the staff alert device worn and is it easily accessible by the employee when in distress? • How is it activated? (e.g. multiple buttons, single button, a pull-string, lack of motion, body in the lying down position, etc.) • How are the real-time location alerts sent? • When an online notification portal is used, what type of alert e.g. audio, visual does it create to alert the responder(s)? • How does the online notification portal display the location of the activated device? 	<p>It is important to understand how the online notification portal/panel will alert the dispatcher/front desk staff, what the staff will see when they view the portal/panel and the ease of defining the location of the activated device.</p>
3.6	<p>Does the solution provide additional (i.e. audio and/or video) communication capabilities so responders can talk to the employee in distress?</p> <p>Describe whether these communications are one-way, two-way, with or without text, audio and/or video and which responders (internal, dispatch, emergency) can participate in the communication method available.</p>	
3.7	<ul style="list-style-type: none"> • How are alerts received and what options are available for handling and escalating alerts? 	<p>As a hotel, it is important to understand how quickly the alerts will be received by the</p>

	<ul style="list-style-type: none"> • How quickly are such alerts received by the appropriate teams? (i.e. immediately, in seconds or in minutes) • Does the dispatcher/front desk personnel/responder have the ability to acknowledge the receipt of the alert? • If someone does not acknowledge the receipt of the alert in a set time frame, is there an escalation process to alert additional individuals? • If escalations are possible, how are alerts sent to additional individuals? 	<p>responders and the capabilities of the system to acknowledge the receipt of such alerts.</p> <p>The ability to acknowledge the receipt of the alert will help with ensuring and enforcing adequate response protocols.</p> <p>The ability to escalate an unacknowledged alert will provide a failsafe in the event that the initial recipient does not respond. This will allow the hotel to be able to measure and guarantee service-level response within the appropriate and obligated time frames.</p>
3.8	<p>Does the staff member carrying the alert device need a smartphone or tablet within a certain proximity for the solution to work? (e.g. tethering or pairing)</p>	<p>Some staff alerting solutions may require additional devices to support the solution. For example, some systems require a smart device to be paired with the alert device.</p> <p>Other solutions may not require a smart device. It is important to understand the implications of this, both from operations/implementation and cost perspective.</p>
3.9	<p>What peripheral equipment (e.g. hubs, beacons) is required for your solution to work?</p> <p>List hardware and indicate if it is either included in your solution, needs to be provided by the hotel or if it can be provided either by the hotel or the vendor.</p>	<p>Given the various approaches, it is critical to understand the solution component (hardware) details around the triggering device, location identification hardware, communication method/hardware, and any on-site servers/equipment.</p> <p>Depending on existing infrastructure, the hotel may opt to leverage existing peripherals in lieu of adding vendor's components. The solution may be capable of leveraging the vendor's peripherals and integrating with existing devices to enhance location accuracy, redundancy, etc.</p> <p>Because staff alerting solutions have different approaches to ascertaining location information, it is important to understand if it's a single source, or correlated with multiple sources, and what happens if location information cannot be transmitted.</p>
3.10	<ul style="list-style-type: none"> • How is peripheral equipment powered? • What is the monitoring, logging and maintenance provision of the power status of the hardware device? 	<p>It is important to consider the power requirements of all of the component hardware pieces of any given solution and how these are maintained over time and how the hotel is</p>

		<p>informed in case the equipment loses power or has low battery.</p> <p>Hotels should also consider the regulations that require or limit the use of certain batteries.</p>
3.11	<ul style="list-style-type: none"> Does a property have to assign one staff alert device per employee or does your solution allow for interchangeable use of the staff alert devices between staff/shifts? If so, is the interchangeable use tracked? 	<p>There are cost and operational considerations that need to be taken into account when determining if one alert device should be allocated per employee, or if an alert device can be shared between employees on different shifts.</p>
3.12	<p>Describe how accurate your proposed solution is to identify the location of an employee with an activated device?</p> <ul style="list-style-type: none"> Include approx. feet, room number, public space, etc. If multiple degrees are available, indicate what is required to achieve the various levels of accuracy Is this solution capable of locating someone both inside and outside of a building? 	<p>Some local ordinances or union contracts may stipulate certain accuracy. It is important to understand how the solution identifies the location of the employee in distress, and at what level of accuracy.</p> <p>Some alert systems can leverage IoT in-room technologies (door locks, set-top boxes, environment controls, etc.) or BLE beacons to ascertain and provide room and correlated location information.</p>
3.13	<p>What are the “covered areas” included in your proposal? (e.g. guest rooms, back of house (BOH), service elevator landings, linen closets, locker rooms, public spaces, meeting rooms, stairwells, elevators, exterior locations, subterranean, garage, beach, golf course)</p>	<p>This will indicate whether the solution can provide coverage in all areas requested by the hotel, including public spaces such as conference rooms, pool areas and golf courses.</p>
3.14	<p>Describe the equipment and devices needed by alert responders at the hotel to receive alert notifications.</p>	<p>This is important because the staff alert solution can be communicated with hotel dispatch, office and management using a range of capabilities, including but not limited to SMS text, API dispatch systems and land mobile radio.</p> <p>Based on the existing environment and policies and procedures at the hotel, one approach may fit better than another.</p>
3.15	<ul style="list-style-type: none"> Does your solution track an employee when the staff alert device is not activated? If so, is this feature configurable to deactivate so tracking is not allowed 	<p>This is important because some local regulations or union Collective Bargaining Agreements (CBAs) may forbid tracking hotel staff during normal day-to-day operations</p>

	<p>when the staff alert device is not activated?</p> <ul style="list-style-type: none"> • May this feature be permanently deactivated or not installed so it cannot be reactivated to track employees? 	<p>when a staff alert device has not been activated.</p>
3.16	<p>Are there any instances (e.g. power outage, internet outage, device tampering, range from associated devices) in which your solution would not be able to identify a staff member's location? If these instances occur do you have an alternative method of identifying a staff member's location?</p>	<p>It is important to know what happens if location information cannot be transmitted and if there are failsafe mechanisms available to determine location.</p>
3.17	<ul style="list-style-type: none"> • Does your solution provide a method to securely self-cancel an alert (e.g. in the event that an employee accidentally activates the staff alert device)? • How do you confirm this is a "true" cancellation and not a cancellation by someone other than the employee? • Can the self-cancellation function be deactivated? 	<p>It is important for hotels to understand the local ordinances and tolerances for responding to false alerts. Some ordinances require that only security personnel are able to reset the device/clear the alarm once it has been initiated.</p> <p>This needs to be balanced with the potential for false alerts: device malfunction, accidental initiating or a call for a non-security related support, which will still require security response and attention.</p>
3.18	<ul style="list-style-type: none"> • What is the duty-cycle (hours, days, years) that the battery will sufficiently power the staff alert device? • If disposable, how often should it be replaced, and what is the replacement procedure, recycling program and cost? • If rechargeable, how often does it need to be recharged, how long does it take to recharge and how many times can it be recharged before needing replacement? 	<p>Consider the type of battery to replace, the tools needed to replace the battery, or, if the vendor provides a replacement service included or excluded with service and maintenance.</p>
3.19	<ul style="list-style-type: none"> • Does the staff alert device communicate its status (e.g. signal strength, battery level, etc.) and if so, how often? • Can your staff alert device notify/report when the battery is low? 	<p>Given that the device is not expected to be activated frequently, it is important to have periodical status updates of the health of the device.</p>
3.20	<p>Is there a way the system can be manually tested to confirm proper functionality of the staff alert device?</p>	<p>Given that the device is not expected to be activated frequently, it is important to have periodical status updates of the health of the device.</p>

3.21	<ul style="list-style-type: none"> Is the staff alert device water-resistant or waterproof? If the device has an IP (Ingress Protection) rating, describe what is covered (e.g. IP-67). 	<p>Buyers should understand how devices can handle the environmental demands of the job. (e.g. bathrooms, chemicals, etc.).</p> <p>The IP Code relates to Ingress Protection rating (e.g. IP-67)</p> <p>More information regarding IP ratings can be found here: https://en.wikipedia.org/wiki/IP_Code</p>
3.22	<ul style="list-style-type: none"> Is the staff alert device impact resistant? If so, what specifications does it meet? 	<p>Durability is especially important given that the device is not used or tested frequently so malfunctions will only be known when an alert needs to be triggered.</p>
3.23	<ul style="list-style-type: none"> Is there a warranty for all of the system components of your solution? If so, how long is the warranty? Please describe the warranty process. 	<p>Understanding the warranty and maintenance inclusions will assist in determining required budgets and the total cost of the solution.</p>
3.24	<p>What is the process for replacing failed or damaged system components and does it differ from replacements covered under the warranty?</p>	<p>Consider whether replacements are shipped in advance, provided through additional on-site inventory, and if inventory incurs additional storage costs. In the case of major component failure, how are they replaced in a timely manner to minimize downtime?</p>
3.25	<p>What local/national regulations/requirements, if any, does your solution comply with? Please provide details of the requirement and how you comply. (Recommend attaching a separate document to identify the specific regulations)</p>	<p>Current compliance with relevant and varied city ordinances and negotiated union contracts is critical. The solution provider should also describe how features can be enabled/disabled or configured to meet various requirements. Also, the provider should describe their program for maintaining compliance as regulatory requirements change.</p>

4 ADDITIONAL PRODUCT INFORMATION

Building upon the foundation of product knowledge, these questions establish a greater context for day-to-day operations when using the solution.

Sample Questions from Buyer to Provider		Question Context and Response Expectations
4.1	Does your solution have a (iOS and Android) mobile application? If so, please describe it.	<p>This question is relevant for staff alert solutions that are smartphone-centric for trigger/fob pairing, communication and location acquisitions support.</p> <p>There may also be apps for the mobile devices that responders carry that will alert them and allow them to acknowledge the alert.</p>
4.2	Does your solution have a web dashboard? If so, please describe it.	It is important to know whether the staff alert solution provides security dispatch with a way to manage staff alerts, acknowledgment, dispatching security resources, escalations or response time reporting.
4.3	How are incidents recorded in your system?	<p>When an alert is triggered, an incident is created and logged in the system.</p> <p>Find out:</p> <ul style="list-style-type: none"> • Where it is logged • How it is reported • If the details are recorded automatically or manually (e.g. time, date, location, venue, room, user, staff member, device)
4.4	Please describe the availability of real-time incident report capabilities as well as historical reports and insights?	Reporting an incident's response time may be required to defend against lawsuits, provide to local regulators that require it, and allow for response time measurement for improving staff alerting response times, training, re-training, and insurance claims.
4.5	Are the incident reports auto-generated or are they required to be downloaded manually?	
4.6	Do you provide a 24/7 dispatch and monitoring service?	Discover if the service is provided by internal resources or if a third-party monitoring service will diagnose the severity of the distress signal and dispatch police and/or EMS? Can dispatch

		rules be modified based on-site staff availability?
4.7	<ul style="list-style-type: none"> Indoor Mapping: Do you have the ability to show the location of the activated device in real-time on a floor plan of the property? Does this include wayfinding? Do you have the ability to reconfigure or update the floor plan of the property? If so, how often does the update occur (e.g. only at the renewal of contract or every "X" years)? 	<p>As a buyer, you may want to have indoor mapping as an alternative, or additional means of representing the location of the alert as opposed to text on a screen.</p> <p>Wayfinding is the ability to find the quickest or shortest path and orient responders within a physical space. Wayfinding in addition to indoor mapping may improve staff alerting response times.</p>
4.8	<ul style="list-style-type: none"> How does your solution check to make sure it is online and working? Does the system send out proactive system warning alerts? 	<p>A range of processes from manual to automatic are supported by staff alert solution vendors. Hotels need to balance cost with solution service level expectations. The higher the service level expectation, redundancy, automation, etc., the greater the cost.</p>
4.9	<ul style="list-style-type: none"> Does the device sound a local audible alarm when activated? If so, how many decibels? Can the alarm be silenced once activated? Can the alarm be set to "mute" as its default? 	<p>Consider local requirements for audible alarms for your properties' such as state and local ordinances, union requirements, etc.</p>



5 DEPLOYMENT & INSTALLATION

This section details how the staff alert devices are deployed and transitioned to a steady state of operations, included key processes, requirements, and estimated durations. This section also covers liability and insurance for both vendors and installers.

Sample Questions from Buyer to Provider		Question Context and Response Expectations
5.1	<p>How is your solution deployed/installed at a property?</p> <p>Describe your pre-implementation, implementation and post-implementation process – include all steps required to implement the solution and transition to a steady state of operations. Be sure to describe any site survey, installation and testing processes. This response may be provided in a timeline, Gantt chart, table or narrative.</p>	<p>The level of effort required to implement staff alert technologies and the implementation process itself varies based on the technology selected. Consider the impact the implementation process may have on your day-to-day business operations. Weigh the implementation process against the benefits of the approach; consider implementation duration, impact on staff resources and impact on guest experience.</p>
5.2	<p>Detail any specific requirements to deploy the solution, including site access requirements (e.g. rooftop access), site resource requirements (e.g. security escorts), and documentation requirements (e.g. list of all the guest rooms).</p>	<p>This information will help the hotelier take into consideration the impact of a vendor's requirements for the deployment of the solution on their day-to-day operations.</p> <p>This also allows the hotel to plan and ensure vendor requirements can be met (e.g. through additional scheduling of escorts, preparing badges and providing materials), which will help to minimize delays or errors during the deployment process.</p> <p>In addition, it is beneficial for a hotelier to assess the opportunity cost of having the rooms out of commission for a period of time during installation.</p>
5.3	<p>If you utilize subcontractors to install or deliver your solution, detail their deployment roles and responsibilities.</p>	<p>Many solution providers utilize subcontractors to deliver their solutions. Consider the role and responsibilities of subcontractors and any requirements you may place on your solution providers' subcontractors (e.g. background screening). Consider whether the requirements change based on whether the subcontractors are on-site or off-site.</p>
5.4	<ul style="list-style-type: none"> Assuming a 200-room hotel requires 30 alert devices, how long (in a number of 	<p>An estimated duration (in a number of days) to deploy for the scenario provided allows ease of</p>

	<p>days) would it take for you to deploy your solution at this property?</p> <ul style="list-style-type: none"> • Are there any variables that can result in a more efficient deployment or in potential deployment delays? 	<p>comparison between different potential vendors.</p>
5.5	<p>If you have any certifications or licenses relevant to deployment of staff alert technologies (e.g. licensed as a security installer), detail them here.</p>	<p>Evaluate if any certifications are a requirement for your solution deployment.</p>
5.6	<p>Please provide information relating to your level of insurance coverage:</p> <ul style="list-style-type: none"> • General commercial liability – in aggregate and each occurrence • Worker's compensation coverage • Automobile coverage • Professional liability • Cybersecurity coverage • Any umbrella coverage • Any other specific insurance that may be required at your hotel 	<p>Hoteliers need to know what kind of coverage a vendor carries in case something goes wrong during installation, service call, product failure, etc.</p>
5.7	<p>Do you conduct background checks on your employees? If so:</p> <ul style="list-style-type: none"> • Do you conduct local state or national background checks? • How many years back does the information go? • Do you conduct ongoing checks? If so, how often? 	<p>This information may be important for a hotel to acquire from a vendor to ensure the hotel meets or exceeds its brand requirements.</p>
5.8	<p>Do you conduct drug testing for your employees? If so, how often?</p>	<p>This information may be important for a hotel to acquire from a vendor to ensure the hotel meets or exceeds their brand requirements.</p>



6 TRAINING

Outlining the training materials, processes and expectations with the below set of questions will enable an evaluation of training resources including the time required and personnel investment.

Sample Questions from Buyer to Provider		Question Context and Response Expectations
6.1	<p>Describe your process and timeline for training hotel staff in preparation for the launch of the staff alert solution.</p> <p>Please provide a link to these materials, if applicable.</p>	<p>This information helps the buyer understand the training process for implementing the vendor's safety solution.</p> <p>This also allows the buyer to assess all employees who are affected and their availability.</p>
6.2	<p>Do you provide on-site training for the staff alert device users? What does this involve?</p>	<p>This is key for the hotelier to schedule their employees, plan shifts and coverage, and to balance the need for training versus executing their day-to-day duties.</p>
6.3	<p>Do you provide on-site training to the staff alert device responders? If so, what does this involve?</p>	<p>This is key for the hotelier to schedule their employees, plan shifts and coverage, and to balance the need for training versus executing their day-to-day duties.</p>
6.4	<p>Provide an overview of your training methodology.</p> <p>Please include:</p> <ul style="list-style-type: none"> • Type of training required (train-the-trainer, traditional trainer-attendee approach) • Training location (in hotel guest areas, on-site training room) • Delivery approach (classroom, online, quick reference card, etc.) • Number of trainees expected to require training • Who will be responsible for organizing/coordinating and conducting training (client or vendor) • Number of training classes for each module expected • Number of trainees allowed per training class 	<p>The investment toward training on the solution is useful to understand and plan accordingly for.</p>

	<ul style="list-style-type: none"> Are there any other resource requirements for training? 	
6.5	<p>Training Materials:</p> <ul style="list-style-type: none"> Who will prepare these materials? What kinds of materials (user/training manual, quick reference card, PowerPoint slides, etc.) will be expected to come out (either created new or modified from existing)? What training resources are available for new managers and employees (post-rollout)? Which languages do you provide your training materials in? 	<p>This allows the hotel to understand what training materials their employees receive and how it fits into their other SOPs (Standard Operating Procedures).</p>
6.6	<p>Is there an online or ongoing training program for re-training or training new employees? Describe what materials are available? If online, please provide a link or copy of materials.</p>	<p>It is important to also consider how the hotel or vendor will provide the training to new employees or retrain existing employees.</p>
6.7	<p>Other Solutions for Training:</p> <p>Do you provide other solutions in addition to the staff alert device solution?</p>	<p>The vendor should describe, as a narrative, what other solutions they provide and how the solution(s) work.</p> <p>The vendor's response will help the Buyer assess the flexibility of the safety solution and whether the other solutions the vendor provides will help with other hotel operations or enhance security.</p> <p>For example, does it include asset tracking, inventory management system, room tray, thermostat, radios, etc.?</p>
6.8	<p>Other Solutions for Training:</p> <p>What connection, if any, exists between these other solutions and the staff alert device solution?</p>	<p>It's important to understand if the multiple product offerings require different platforms, different apps, different hardware or if they are all part of the same platform, how they work together.</p>

7 TECHNICAL QUESTIONS

Describing the infrastructure required for a solution, along with other technical questions from this section, allows the Buyer to better understand the impact the solution will have on the property.

	Sample Questions from Buyer to Provider	Question Context and Response Expectations
7.1	Describe the infrastructure required at the hotel property for your proposed solution to work.	Helps you assess what you need at your property or anything you may need to purchase to implement this solution.
7.2	Are servers required on-premises or provided through cloud-based services?	Hotels will need to plan space, maintenance and additional costs for any on-premise hardware.
7.3	<ul style="list-style-type: none"> • If servers are provided through off-premise/cloud services, where are the servers hosted? • Is there any redundancy to those servers or options for backup communication? 	The reputability of the hosting service should be considered in addition to other technical conditions in this document.
7.4	If servers are provided on-premise, who owns and is responsible for the hardware, the warranty, support and maintenance? Are there additional costs for on-premise server hardware and any associated services?	It is important to know for total cost of ownership: resource allocation of space, staff resources, power, cooling, etc.
7.5	Please provide a list of relevant IT compliance and security certifications of the hosting environment – (e.g. SSAE1, SSAE16, ISO27001, ISO/IEC 27018:2014, PCI-DSS Compliance)	The list of certifications provided by the vendor will assist the buyer to evaluate the reliability and stability of the vendor's hosting environment. Note: Not all of these example certifications may apply. Consult with your IT department to identify appropriate certifications to ask for your situation.
7.6	<ul style="list-style-type: none"> • What Service Level Agreement (SLA) is available? • If there are different levels of reliability, what points of failure exist under the SLA? 	SLA metrics should include uptime availability, latency and mean-time to repair.
7.7	How does your solution maintain constant functionality?	This may help find any gaps between what the solution needs and the capabilities of your infrastructure.

7.8	<ul style="list-style-type: none"> • Are there planned service interruptions? • If so, at what frequency? 	This will help plan and manage during service interruptions especially when service interruptions take longer time than you anticipate or tolerate.
7.9	<ul style="list-style-type: none"> • Do you collect Personally Identifiable Information (PII)? • If so, what is the main use of the personal data in your solution? 	Staff users and responders may register their names and phone numbers in the system, so it is important to know how this information is stored and processed. Additionally, reported incidents which may include names and details could also be considered PII.
7.10	Do you perform vulnerability scanning or penetration testing every year?	This is useful for illuminating unknown security weaknesses and to know if the solution offers fixes to security problems.
7.11	Is personal and confidential data encrypted in the database level in your system?	This is important to meet compliance mandates and keep business assets protected.
7.12	Does your system have role-based access levels?	This is important to ensure users are only able to access data relevant to their role.
7.13	Does your solution support Single Sign-On (SSO)? If so, what SSO standards are compatible?	This is important because it can minimize administrative overhead if SSO is compatible with existing user authentication mechanisms.
7.14	<p>What are the available user authentication processes?</p> <p>Include SSO support and standards compatibility, configurable password requirements, uniqueness, complexity, self-service password reset, password change notifications and bad password attempts.</p>	<p>This helps the buyer trade-off between the needs, strength of authentication, cost and ease of operation.</p> <p>For example, while use of a username and a password is a simple authentication process, a two-factor authentication involving a verification code received via text message on a preregistered mobile phone is a more robust method.</p> <p>Machine authentication through digital certificates may be needed for online backup services, patching and updating systems and remote monitoring.</p>
7.15	Is your application able to provide a user activity report when reports are generated, files are downloaded or data is exported?	This is necessary for data loss prevention.
7.16	What anti-malware, firewall, intrusion prevention and detection systems are used to protect the applications and the data in your solution?	This is important because anti-malware and system/software needs to be updated constantly as new threats evolve. Besides,

		<p>anti-malware software may rely on reputation-based systems.</p> <p>Depending on the infrastructure you have, it is important to know if the firewall intrusion prevention solution supports on-premise server or cloud-connected networks.</p>
7.17	<p>What data encryption methods are leveraged in your proposed solution?</p> <p>Include Wi-Fi encryption (e.g. WPA2, WPA3), Internet encryption protocols (e.g. TLS, SSL) or any other wireless standards such as Bluetooth, Zigbee, Z-Wave, etc.</p>	<p>Depending on requirements, encryption may or may not be required for every communication process but should be included for any Internet-based communication. For example, between the property and a cloud hosting service or third-party monitoring service.</p>
7.18	<p>Describe the backup and restoration process for your systems.</p>	<p>This may not be relevant to cloud-based systems, but on-premise systems may have an automated process that should be verified and tested regularly.</p>
7.19	<p>What is your current data retention policy, and can it be modified?</p>	<p>You may have different data retention requirements than the default, so modification may be necessary.</p>
7.20	<p>Describe the Service Level Agreement (SLA) and response times for system downtime of the support services.</p>	<p>Consider whether the SLA meets your requirements and risk tolerances.</p>
7.21	<p>What is your process of notifying the property in case of any system breach?</p>	<p>It is important to understand if there is continuous monitoring of the system and automatic notification to the stakeholders of the property. Does the notification contain a type of breach, does it include any resolution, any necessary steps to be taken, etc.?</p>
7.22	<p>Describe the types of data transmitted to you or to any other provider/partner from your solution.</p> <p>If transmitted to another provider/partner, detail the reasons for why another provider would receive such data and how that data is protected from a breach/corruption.</p>	<p>This is important from the point of protecting confidential information and liability.</p>
7.23	<p>Does your solution integrate directly with local law enforcement/emergency response or third-party security monitoring and dispatch?</p>	<p>Consider the ability of the solution to escalate alerts to off-site responders. Some factors to consider include location of the property, response times of the responders,</p>

		the type of property and if on-site responders are available at all hours.
7.24	Please attach a copy of your current information security policies and standards.	Some vendors may claim it is proprietary, but you should know if they have one.

8 ACCOUNT MANAGEMENT & SUPPORT

This section provides context for support and resources for the proposed solution. This includes account management, escalation of issues and vendor management of performance post installation.

	Sample Questions from Buyer to Provider	Question Context and Response Expectations
8.1	<p>Describe your customer account management and client success program. (i.e. KPI's, review schedule, or ongoing client engagement process).</p> <ul style="list-style-type: none"> • Include a statement that explains the process that will take place once awarded the contract. • This should also include any points of escalation and a hierarchy diagram. Within this statement there should also be a section clearly stating the number of reviews (interim, annual, monthly, periodically) that will be held with the vendor and what the purpose of these reviews will be. • Provide details of how the performance of the solution is measured once installed and provide issue/resolution statistics, details of dashboard reporting etc. 	<p>It is important to know what resources are available should the buyer need assistance, and how the vendor will monitor the solution to ensure its success.</p>
8.2	<p>How many resources does the vendor have in specific roles available to service the buyer's account (i.e. headcount dedicated to sales, on-site support, remote help desk support, R&D)?</p>	<p>It is useful to understand the scale of a company's support function, and whether the level of account support fits the buyer's needs.</p>
8.3	<ul style="list-style-type: none"> • What regions do you have resources in? • What regions can provide customer support services? • Would the resources be remote/telephone and/or be local/onsite? 	<p>It is useful to understand if the geographic presence of the provider matches your geographic property footprint.</p>
8.4	<p>What language(s) does your help desk/support speak?</p>	



8.5	What are the regular support service hours and time zones for your help desk/support and escalation?	This is important to know if support service will be available during or outside of the buyer's local business hours, as hotels operate around the clock 24/7.
8.6	Please describe the escalation process for a standard and critical system outage, hours of availability and related response times during and outside of regular hours.	Depending on the type of system outage, some escalation methods may not work. For example, when the network goes down, chat and email escalations may not go through.



9 INTEGRATION

This section will help the buyer assess whether the vendor's staff alert solution is a stand-alone solution or if it has the ability to integrate with the buyer's other existing or prospective systems. Such integrations may allow for enhancements to the staff alert solution or additional features such as integrated reporting.

	Sample Questions from Buyer to Provider	Question Context and Response Expectations
9.1	<p>Can your solution integrate with third-party applications?</p> <p>If so, list your solutions integration capabilities by identifying which existing infrastructure elements your solution supports, and which manufacturers you integrate with. (For example, door lock systems, thermostats, room control panels, etc.)</p>	<p>This is important because it will tell you if the proposed solution is compatible with your existing infrastructure, or if changes will be required.</p> <p>The vendor's response will also tell you how their solution might integrate with other systems within your hotel.</p>
9.2	<ul style="list-style-type: none"> • Does your solution integrate directly with first responders? • If so, is there a configurable escalation process? 	<p>It is important to know whether the system will automatically notify first responders (such as the police or fire department), or if it is up to the hotel's personnel to notify first responders, as deemed necessary.</p>
9.3	<ul style="list-style-type: none"> • Does your solution integrate with a service optimization system? • If yes, which products do you integrate with? <p>Indicate whether the proposed solution allows integration or <u>requires</u> integration into a service optimization system.</p> <p>Provide the name of the manufacturer and level of integration that the system provides, and indicate the benefit achieved by the integration.</p>	<p>It is important to know if integrations are optional or mandatory and to what level solutions are integrated.</p>



10 UPGRADES

This section will provide the buyer with expectations regarding the solution upgrade lifecycle for both software and hardware.

Sample Questions from Buyer to Provider		Question Context and Response Expectations
10.1	<p>How often will the staff alert solution be upgraded or updated?</p> <p>Please provide an upgrade process summary.</p>	<p>It is important to understand the expected lifecycle of the staff alert solution, as well as if (and how) the vendor will add new features to this solution.</p>
10.2	<ul style="list-style-type: none"> • How do system upgrades or updates impact normal hotel operations? • What type of notifications are provided prior to these upgrades and updates? • Are updates performed on-site or remotely? 	<p>A hotel needs to know how many resources they will have to put into maintaining the solution.</p> <p>The hotel's workload will vary depending on if updates happen on-site or remotely, impact hotel operations or require the system to shut down.</p>
10.3	<p>For <u>planned</u> system upgrades or updates, how will the property be notified in advance?</p>	<p>This will clarify how a vendor will notify the property of an update and what the related procedures are for a planned update.</p>

11 SCALABILITY

This section focuses on whether the vendor can meet the buyer's needs across different regions, nationally or internationally, if needed. This also allows the buyer to assess the vendor's ability to deploy in hotels of various sizes.

	Sample Questions from Buyer to Provider	Question Context and Response Expectations
11.1	Describe how the staff alert solution will scale regionally, nationally, and internationally to meet the needs of your hotel brands.	<p>Depending on the size and scale of the hotel entity, it's important to understand a system's ability to scale, be installed and serviced on a regional, national and international scale.</p> <p>The hotelier may request a coverage map and list of countries that a vendor can support to better understand the vendor's reach today or in the future.</p>
11.2	Does the staff alert solution support small (<100 rooms), medium (100-500 rooms) and large scale (500+ room) properties on the same platform?	<p>Discover what the scalability limits (if any) are of the staff alert solution and if it can scale from small to large properties on the same platform.</p> <p>Find out if there are any limitations or upgrades that may be needed to support the relevant hotel sizes.</p>

12 PRICING

This section allows the buyer to assess all costs, including but not limited to, up-front costs, annual subscriptions, installation fees, and other ongoing costs a buyer may incur through the lifespan of the staff alert solution.

	Sample Questions from Buyer to Provider	Question Context and Response Expectations
12.1	Provide first year or initial rollout costs in US dollars: <ul style="list-style-type: none"> • Equipment purchase cost • Installation cost • Professional fees – what is included, such as training • Estimate travel costs • And any other set-up costs 	Understand the components of pricing which include hardware costs, installation fee, software subscription, licensing fees, training costs, travel costs, and any other set up costs that may be involved in launching the product.
12.2	Provide details for ongoing costs to the property including: <ul style="list-style-type: none"> • Annual service/maintenance cost per unit • Software licensing fees • Hosting costs 	Learn what the ongoing costs are, which may include a subscription fee, licensing fee, ongoing training fee, hosting costs, updating indoor maps or an onsite support fee.
12.3	Provide details for any cost of replacing equipment, including alert devices, batteries, etc.	This will provide insight to the ongoing costs of replacing the equipment and consumables of the solution.
12.4	Are there any other additional fees? This may include the cost for 24x7 support, customization costs, integration fees, on-site support billing, etc.	Learn if any additional costs should be taken into account for budgeting.
12.5	<ul style="list-style-type: none"> • Are the prices capped? • If so, for how long? • Are price increases index-linked? Please specify which index (e.g. Consumer Pricing Index). 	Understand what a buyer can expect in terms of year-over-year pricing changes that may take place. Learn how often the vendor typically changes pricing and how new products or features may be priced?



13 CONCLUSION

There is a lot to consider during the search for staff alert technology suitable and complimentary to your hotel, group of hotels or overall hospitality brand. A vast group of hoteliers, technology vendors and independent consultants, combined their expertise and built out this Buyer's Guide to help organizations currently going through the process of buying staff alert technology.

This Buyer's Guide, while as comprehensive as possible, may not address all the potential concerns of a hotel or brand of hotels. In addition, these questions may even spark additional questions for a Buyer.

Independent consultants are a valuable partner in making this selection process meet the needs of hotel operators, owners and their employees. HTNG recommends working with an independent consultant for further recommendations or guidance. HTNG maintains a public directory of qualified consultants available to assist groups in various sectors within hospitality technology. This list can be found at: <https://www.htng.org/page/ConsultantDirectory>.



14 APPENDICES

14.1 GLOSSARY OF TERMS

For the purpose of this document the following terms have been defined as follows:

Term	Definition
KPI	Key Performance Indicator: measurements a company can use to gauge its performance over time.
R&D	Research and Development
SLA	Service Level Agreement: a commitment between service providers and clients involving aspects of the services provided.
SSO	Single Sign-On: allows access to multiple software systems using one login
PII	Personally Identifiable Information
SOP	Standard Operating Procedures
Wayfinding	The ability to find the quickest or shortest path and orient responders within a physical space
IP-Code	Ingress Protection: protection ratings against moisture and fine particles. (e.g. IP-67)
CBA	Collective Bargaining Agreement: a labor contract agreed upon between management and trade unions
IoT	Internet of Things: Internet communicating physical objects, devices, and sensors
BLE	Bluetooth Low Energy: a wireless personal area network technology aimed at applications in healthcare, fitness, security, and more
WBE	Women Business Enterprise
MBE	Minority Business Enterprise
SDB	Small Disadvantaged Business
FEIN	Federal Employment Identification Number, also known as a Tax ID