Invision security
The Power Behind Protection

EXPERT SERIES

RFP TEMPLATE: **CAMPUS SAFETY**

The IT Pro's Blueprint for Writing a Campus Safety RFP

RFP TEMPLATE: CAMPUS SAFETY

Introduction

Campus safety and security technology are at an inflection point. There's widespread uneasiness regarding safety among students, staff and parents. Ongoing incidents of active shooters and other threats have escalated and the public and private sector is struggling with how best to handle what now seems like a formidable challenge related to educational facilities. Writing a request for proposal (RFP) for technology is difficult, because there are so many moving parts and stakeholders on a campus, including the surrounding community as well as local law enforcement and private citizens if an urban setting.

The security industry's goal to deter, detect and delay is still a critical building block. But as active shooters have become a recurring theme, the Department of Homeland Security's Ready.gov website has recommendations to "Run, Hide, Fight." School administration and students are conducting safety preparedness drills to proactively address the potential for shootings on campus and lock downs are increasingly deployed in tandem with technology solutions. Now more than ever, protecting campuses and students takes a holistic approach, starting with a risk assessment, site survey and review of all historical data pertaining to

past incidents on or near campus.

Many different stakeholders need to collaborate in developing an effective security posture for the campus. There's the school administration, security integrator, IT department, local law enforcement, campus police, door consultants, architects, specifiers and others who all need to weigh in with their expertise in order to develop the most effective proposal for the future. There are numerous technologies to consider, but these should only enter the equation after the primary goals and objectives for the campus safety solution are determined. Because campus threats have changed and morphed with the times, there are new and emerging technologies to consider, such as gunshot detection and two-way voice systems. There's also the need for emergency duress notification for parking garages and other spaces.

There are so many other different technologies available, including access control, video surveillance, lighting, emergency and mass communications, wireless and hardwired locks, two-way communications, intrusion detection, bullet and blast resistant materials, metal detectors, man traps for entrances as well as the communications and network infrastructure. A holistic approach with technologies piggybacking off each other offers the best mitigating pathways—but how do these parts and pieces get integrated effectively? And how do they communicate or interface with local authorities in addition to campus police if applicable? What about visitor management systems for staff and teachers and how does this play into the overall security plan? There's also the process of Crime Prevention through Environmental Design and creating manmade and natural barriers to discourage attacks or other surreptitious activity on campus. Campus safety is also about policy and procedures, people and their roles as well as adhering to codes and regulations on campus, including The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act, the Americans with Disabilities Act for equal access as well as others.

The campus safety RFP needs to be a highly detailed document that proactively addresses current or emerging threats. Like other security processes, it necessitates a layered approach that hardens the facility from the outside in, coupled with procurement of technology that minimizes risk and builds upon other solutions.

Collaborate with Others

Conduct your research well ahead of the RFP so you can tailor it as closely as possible to the ultimate goals and needs of students, teachers, staff and all stakeholders. Talk to other security end-users at schools or campuses with similar challenges or characteristics. Conduct fact-finding workshops with manufacturers, consultants, architects and systems integrators prior to the RFP if possible. Do your homework and thoroughly investigate current and emerging technology. Get buy-in from the student population and conduct surveys on how they feel about video surveillance, access control, lock down and even gunshot detection.

Pull Quote

Remember that others have gone through this experience and you may be able to gain valuable information from their successes or failures.

A proactive plan requires additional deep-dive into your campus and the way it works on a day-to-day basis. The potential service provider needs as much information as possible to streamline the process and design with your end goal in mind. Unless the person writing your RFP is an expert, you want to make sure you've engaged a qualified consultant to talk through your risk profile, help you understand best practices and ultimately learn how you can properly apply the right technology for your campus.

We've assembled a list of open-ended questions that, once answered, will allow you to address primary areas of consideration in constructing your RFP for a campus safety and security project. These questions are an effort to cover the major areas a provider will need to know in order to form a bid for the service project. Answer these questions candidly and thoroughly and involve other decision makers in order to assemble your RFP as accurately as possible, so the service provider can also respond with a targeted tailored plan.

Campus Background

1. What is the mission, objective and educational philosophy of our university or college and who at the top role(s) should be involved in this process?
2. What is our geographical area of coverage (local, regional, remote locations or satellite campuses)?
3. What buildings and facilities will require security and/or communications?
4. Is this new construction or retrofit and if retrofit what are the characteristics of the building(s)? If new construction what might be the timeline or other challenges or considerations during installation, such as working when school is in session?
5. Are students living on-campus or are we primarily a commuter facility?
6. Are dormitories part of our campus and what are the specifics related to those facilities as far as number of buildings, number of students, existing security?

7. What are additional critical details about the physical space(s) in which the campus is located and past security incidents that have occurred?
8. Have we conducted a site survey, security audit and risk assessment in the recent past and what were the results?
9. What is our risk, compliance and security posture? What current security policies and operating standards are in place for physical security technology?
10. Have reports on campus incidents been reviewed for the last several years and what were the results/conclusions?
11. Have we reviewed and charted local crime data and statistics?
12. What kinds of doors and locks are installed and how will they play into the new/upgraded specification?
13. What is the landscape of installed systems, including access control, surveillance, intrusion detection, intercoms and paging or mass notification/emergency communications?
14. What is the base of legacy solutions that will be upgraded or replaced and/or will migration and longer-term strategies be necessary?
15. Will access control systems or visitor management be part of the new solution and will it integrate with intrusion detection, surveillance, time and attendance or other installed technologies?
16. Will we require single points or multiple points of entry?
17. Who ultimately will be responsible for the system? How will it integrate with our existing command center if applicable? What about with local law enforcement or campus police?
18. Will we require reasonable accommodation for the handicapped to ensure compliance with the Americans with Disabilities Act (ADA)?
19. Will we be relying on grants or other mechanisms to fund the project?

Project Overview

20. What are the most important features and characteristics we are looking for in our purchase and installation or upgrade of the campus solution?
21. What are our project's primary objectives and overall what should our solution accomplish?
22. Who are the primary stakeholders? Campus safety director, security manager, facilities manager, local law enforcement, school administrator, systems integrator, door and hardware consultant, IT director, specifier, architect, consultant?
23. Will social media be monitored to identify risks and how will that integrate with security notification and campus communications technology?
24. What specific offsite locations or satellite campuses require security? What about remote parking garages or locations?
25. Is there an onsite security operations center for monitoring and will security also be monitored there, in the cloud or through a third-party central monitoring facility?

Pull Quote

26. What specific threats or recent security incidents have been identified as a failure or potential failure of the physical security solution and how do the proposed technologies play into a remedy for that lapse?
27. Will we require lockdown capability and where specifically?
28. Is real-time communications to the access control or other systems a critical requirement and for perimeter doors only and/or interior ones?
29. Are there high-security areas where two-factor authentication might be required, such as a combination of card, PIN or biometric verification?
30. How will after-hours access be controlled and managed?
31. Is data collection required by the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act and the Higher Education Opportunity Act?

Existing Environment

32. What specific brand(s) of security technology products/systems/services have been purchased and deployed in the past if any? Will this RFP upgrade or incorporate new technology?
33. What is the communications backbone for the school and will security products piggyback off that? What about the network—will we need to build out a new network or can we use an existing network, segmented, to deploy technology?
34. Will equipment be networked and how/will it be shared with local law enforcement or campus security and safety?
35. What kinds of credentials will we require for access control, such as cards, identification badges and smartphone apps? What about keypads, PINs or biometrics for multi-factor authentication for high-security or sensitive areas?
36. Are smart cards currently being used for security and debit on campus?
37. Is there a guard on duty at specific locations or available on demand? Do they perform guard tours or will video surveillance be needed for that functionality?
38. Will we require logical access control for computers or data centers?
39. Will the system be hardwired or wireless or a combination of both? Are the buildings historical or will the structure prevent drilling or otherwise necessitate a wireless approach? Will a hybrid system work—hardwired in some locations and wireless in others?
40. How is signal penetration in the building(s) and has a wireless signal strength study been conducted?
41. What is the makeup of our current network system so providers know what they need to build around or into?
42. Will the access control, camera or intercom solution be IP in nature and how will we want it segmented on the network? Will we build out a separate network?
43. If considering IP, what is the network coverage and has a formal study been conducted? Do we have IP connectivity drops available where necessary or will they need to be added?

44. What is the specific configuration of the network? Is it cloud-hosted or on-site servers? VPN? IPV4 versus IPV6?
45. Will we desire to work with an outside consultant in the deployment and for ongoing execution and management or do we have staff members with expertise to assess and implement proposed products and services on an ongoing basis?
46. What technical expertise do we have on campus to help execute the contract—CSO, CIO, IT technicians, facility executive managers, others?
47. Have we completed a physical security risk and threat assessment and what was the date/results?
48. What other compliances and regulations must be addressed and adhered to?
49. Will the solution meet National Fire Alarm and Signaling Code NFPA 72 and NFPA 101 Life Safety Code as required for egress?

Service Expectations

50. Will we need to execute a monthly or annual service agreement contract to maintain the system? Or will this be a project-based bid only?
51. What will we expect from the provider in terms of ongoing service?
52. Does the potential installation provider offer managed services; what features are available and what is the approximate monthly cost?
53. Will annual, semi-annual or quarterly system testing be performed with documentation?
54. Will we require compliance and regulatory assessments and at what intervals?
55. What is our budget, timeline, when the provider can work on the project (during school sessions, at off times or other constraints)?
56. Who is our designated security project manager who will be involved in the process (include the name and title in the RFP)?
57. Will the potential service provider agree to sign a non-disclosure agreement?
58. What is our deadline for responses and what is the contact information for whom the proposal should be sent to?

We at My TechDecisions understand that writing RFPs is a critical component of your job but also one of the most dreaded. That is why over the past year, we have created a series of guides to help define your needs and then actually write the RFP. These resources cover a total of nineteen different solutions, including: access control, audio, building control & automation, campus safety, cloud email, collaboration, communication, cybersecurity, digital signage, energy management, hardware, interactive whiteboards, networking, projectors, storage & backup, videoconferencing, video surveillance, video wall and VoIP. You can see our entire library of RFP resources at: mytechdecisions.com/rfp