STANLEY Security

5 CRITICAL COMPONENTS **OF YOUR CAMPUS SECURITY PROGRAM**

At STANLEY Security, we collaborate with hundreds of university partners on their security projects and programs. Each of these partnerships has taught us lessons about how to approach these implementations and serve in these environments.

Being successful in these large deployments means having the strength to overcome, change and adapt to the challenges that arise as needed, as well as a plan to mitigate those possibilities. It does matter who your security partner is, as they must have the agility needed to meet these challenges.

This document reflects the myriad lessons we've learned from our experience partnering with colleges and universities. From something as daunting as thousands of wireless locks dropping offline on Move-in Day to something as seemingly minor as having the wrong parking permit type. If something has gone awry, we've likely seen it.

But as with most things in life, challenges often provide significant opportunity to learn and grow, and we – along with our university partners – have discovered some best practices and considerations for securing institutions of higher education through these collaborative journeys. Below, you'll find many of these compiled into the five critical components of a campus security program.

ROLES AND RESPONSIBILITIES

When launching a large-scale security project, roles and responsibilities both internally and externally must be defined from the start. Institutions of higher education are incredibly complex and interdependent ecosystems that thrive on structure and partnerships. Collaboration is paramount to implementing systemic changes affecting all campus stakeholders.

Oftentimes, we see with large upgrade or migration projects that certain representation is neglected in the preparation and activation of campus changes. Building a list of stakeholders at the project's onset helps mitigate potential misses in project planning.

You should consider including representatives from the following functions and departments:

- Senior leadership
- University police/public safety
- Environmental health & safety
- Emergency response team
- Code compliance department
- Facilities/operations
- Lock shop
- Electrical shop
- Power users/system administrators (people required to interact with upgraded system on a regular basis)
- Information technology
- Legal
- University departments (Housing, Athletics, Academics, etc.)
- University Services (parking, campus dining, campus stores)
- Capital planning
- Student government/student representation
- Procurement
- Security integrator
- Third-party housing partners
- Campus vendors/contractors (any additional external parties required to complete tasks)

COMMUNICATION

Many higher education institutions invest significant money in upgrading technology but lack a communication strategy or infrastructure in place to support it and drive adoption. The best way to approach security program implementation is to start by developing a comprehensive communication strategy. This is can be the critical difference between success and failure.

First, leadership should communicate the value of this project to the entire campus. Those involved must understand the value proposition in order to limit resistance to change and optimize the implementation and ongoing security strategy. Leaders must consider the following:

- Has the university communicated this project to the broader community?
- Are campus stakeholders aware of why security integrator representatives (project managers, subcontractors, technicians, etc.) are in their buildings?
- Are the correct individuals "in the know"?

Another critical component is using the right communication method for each piece of information. Consider what information is shared to whom and how often that information is shared. More than likely, you will have a varied approach depending on which stakeholders need to be informed of what. The project team may have daily progress meetings and email updates, whereas an executive update may only be necessary weekly or monthly.

This also means reviewing the form of communication used depending on the response time needed. For example, we've found that once testing begins, radios are the best technology to use to reach other team members, as cell phones often lose signal in the depths of building basements and run out of battery quickly – not ideal when you are testing a safety or security system.

Having open lines of communication, a regular reporting cadence and the right stakeholders at the table will allow for the quick resolution of issues and support campus-wide adoption.

DOCUMENTATION CONSIDERATIONS

As you begin your campus security project, there are various documentation considerations that must be accounted for before diving into implementation. These documentation protocols will allow your project team to transition into the installation phase smoothly and effectively, ensuring each member of the team is on the same page throughout the entire process – from having a documented process for escalating issues to sharing standardized progress and testing reports.

- Clearly identify all specialized clearances or training required for on-campus work
- Clearly define roles and specify escalation measures
- Clearly define existing system responsibility and response expectations
- Thoroughly review all existing documentation (wiring diagrams, process workflows, naming conventions, device maps, software integrations, installation standards)
- Establish documentation and standardization of the following:
  - Hardware naming convention
  - Software naming convention
  - Physical device labeling
  - Physical device wiring requirements
  - As-built drawings
  - Hardware testing documents
  - Software testing documents
  - Commissioning procedures
  - Testing and acceptance procedures
  - Progress reports
  - Change order request forms
  - Detailed installation standards (wiring preferences, establish if end-to-end supervision is required, preferred panel cabinet layout, signage)
  - Workflow documentation for software integrations: Is this available or will this need to be built as part of the project?
  - Punch list and close-out documentation
  - AIA forms (if needed)

STANLEY Security

PLANNING & IMPLEMENTATION

With the project team's roles and responsibilities established and working standards defined, you and your security integrator will be prepared to plan and implement your security solutions.

Planning

Planning includes a detailed review of your new or upgraded security solution and how its components will be implemented on your campus. Your integrator should give special attention to certain steps in the plan, including:

- **Scheduling:** When you plan for security system migrations and upgrades on campuses, you'll uncover a host of unique challenges, especially around timing. Access control projects, in particular, can be the most disruptive types of projects to a university if they're not carefully scheduled with a host of backup plans. In many cases, you are changing how someone enters a building, so you must fully understand occupancy scheduling, the needs of all departments and proper testing requirements.
- **Accessibility of campus resources:** The implementation process will require on-campus resource use like power consumption, network drops or use of campus pathways. Your security integrator will need to work with departments such as IT, Facilities and Construction to arrange for any needed resources.
- **Aesthetic considerations:** Many campus buildings have historic prestige that should be preserved, or they possess other aesthetic qualities important to your community. Your integrator should plan around those needs as they add or upgrade your systems.

Implementation

With a plan in place and documentation established, it's time for project delivery. While the installation and implementation of new security elements matter most, you should also consider what processes you'll need while the work is being done. From the first device installed to the go-live date, delivery processes will ensure your project team is operating smoothly.

- **Establish daily process protocols:** This includes establishing the sign-in/sign-out process, building a contact list, securing required parking permits, identifying areas where university escorts are required and more.
- **Establish testing environment (highly encouraged):** Will the university provide a testing environment complete with downstream devices or should the vendor do so? In addition to the test environment, have you accounted for ongoing software support for this test environment and corresponding integrations?
- **Define cutover/go-live milestone date plan:** Build a plan to include extra staffing/supplies, clear communication and defined roles, including the creation of a field team and head end team. Additionally, establish a central meeting space for all relevant parties (typically located at an Emergency Operations Center, Security Operations Center or Incident Command Center).

Throughout the implementation process, your security integrator should provide updates at regular intervals and offer opportunities for feedback and discussion on the plan's progress. While they'll work with you to ensure they identify all potential issues up-front and before work begins, even the best-laid plans will require alterations during the implementation phase. New needs arise and new challenges present themselves. An experienced integrator will be able to manage these changes as they arise and work with you to resolve them successfully.

COMMUNITY ENGAGEMENT

Success in higher education security projects is often determined by how quickly external partners assimilate into the community in order to understand its unique aspects and values. The sooner they can fully appreciate the different dynamics of the campus, the sooner they can advocate on its behalf and truly provide thought leadership benefits to the institution.

Here are some ways STANLEY Security has partnered in the past with campuses to build out meaningful relationships and outcomes.

- **Move-in crew –** For move-in days, especially when new access control technology is being deployed, we've partnered with university housing welcome teams to assist students and parents with unloading belongings and operating any new access control credentials or devices they may not be familiar with. Move-In Day is stressful enough without having to figure out how to access your residence hall room.
- **University events –** Whether at an athletic event tailgate or a senior day BBQ, we've leveraged our Stanley Black & Decker sports partnerships to bring assets (NASCAR, MLB, PBR, Extreme Sports) to engage with the community and have fun.
- **Student paper –** When implementing significant system changes that will alter the student experience, we've helped co-author communications with the project team for the student paper and residence life social media accounts.
- **Career fairs –** Stanley Black & Decker is always recruiting talent across all of our business units and functions. Attending the career fairs of our university partners is a fantastic opportunity to recruit top additions to our team and help students land a job right out of college.
- **Clery Act and Title IX professional development opportunities –** We've hosted several Clery Act and Title IX trainings for university partners at no additional cost to the university. This is an opportunity for our customers to benefit from additional education from our partners that will help them better understand requirements and protocols surrounding their university.
- **Strategic pilots –** As new safety and security technologies come to market, involving strategic higher education partners in collaborative pilots has proven to be a mutually beneficial experience. It gives us the opportunity to evaluate potential customers' needs and gives the university an understanding of how the industry is continuing to hone safety and security measures for campuses.
- **Innovation partnerships –** STANLEY Ventures is a global team looking to invest in promising start-up relationships. A key part of innovation partnerships comes from university incubator programs. Where we can connect both parties for interesting conversations, we do.

CONCLUSION

As you begin planning how you want to make your campus more secure, we hope these best practices help you prepare the best standards and processes for the long but important journey ahead. With these five critical components in place, you can work with a partner like STANLEY Security and implement your campus security project with confidence. Your partner can guide you through this process and help resolve the issues that arise during these large deployments. Together, you can create a safer campus environment for your students and the members of your community.