THE UNIVERSITY *of* NORTH CAROLINA
GREENSBORO

Business Affairs

254 Mossman Building
PO Box 26170, Greensboro, NC 27402-6170
336.334.4080 *Phone* 336.334.4754 *Fax*

MEMORANDUM

TO: Chancellor Franklin D. Gilliam, Jr.

FROM: Charlie Maimone, Vice Chancellor for Business Affairs

DATE: January 25, 2017

RE: **UNC Greensboro Master Security Plan**

As part of the ongoing commitment to create a safe and secure environment for students, faculty, staff and visitors, staff representing Environmental Health and Safety, Facilities and University Police, led by Chief Lester, conducted an audit of campus infrastructure, buildings, facilities and open spaces.

The 2017-2020 Master Security Plan provides a unified, comprehensive strategy to enhance the safety and security of the campus; and strategic and operational directives designed to mitigate existing risks, educate the campus community and deter criminal behavior. The Plan's risk management strategy will promote a safe and secure environment as the university infrastructure and facilities evolve over time.

The Master Security Plan was completed in December 2016. Based on quantitative data, risk assessments and extensive interviews with members of the University community, it will provide a comprehensive roadmap for UNC Greensboro to further its security initiatives and improve safety.

The document is attached for your review and approval before introduction to the campus community or making it available to the public.

The plan is also available at the following link:
https://docs.google.com/document/d/1pnWifsXzXahe4_EIl_JX2udzlnZCzWXbPRaNHhJxk7o/edit

Thank you for your consideration of this request.

Executive Summary

As part of its ongoing commitment to create a safe and secure environment for students, faculty, staff, and visitors, The University of North Carolina at Greensboro (UNC Greensboro) has conducted an audit of campus infrastructure, buildings, facilities, and open spaces. The 2017-2020 Master Security Plan provides a unified, comprehensive strategy to enhance the safety and security of the campus.

The Plan provides strategic and operational directives designed to mitigate existing risks, educate the campus community, and deter criminal behavior. The Plan also provides a risk management strategy that can be used to maintain a safe and secure environment as university infrastructure and facilities evolve over time.

Challenge - Managing New Regulations, Growth, and Use of Security Technologies
In an effort to strengthen physical security on university campuses, the U.S. Congress has passed several pieces of legislation over the past decade stipulating new regulations, policies, and reporting practices. This new legislation requires close coordination among multiple programs and offices, meticulous data collection, diligent reporting of incidents, adoption of new policies and procedures, training mandates, and upgrades to security technologies and infrastructure.

In addition, over the past several years UNC Greensboro has adopted practices and implemented programs to enhance security on campus. Significant growth over the last decade in both the population and the campus physical environment has resulted in the need to more efficiently manage security resources to establish a coordinated, effective and collaborative security program.

It is important to develop a sustainable and scalable financial model to support the investment in security personnel, technologies and infrastructure to meet evolving campus security needs.

The Master Security Plan
This Master Security Plan will enable the University to develop a comprehensive strategy to enhance security on campus. The Plan provides:

- A strategic plan to enhance the safety of students, faculty, staff, and visitors and to protect University property
- A targeted assessment of security at UNC Greensboro
- A 4-year implementation plan, including budget and timeline

This Plan does not address strategies for enhancing information and network security; cyber security will continue to be wholly managed by the University's Information Technology Services division. Throughout this Plan, the term "security" shall be interpreted to mean "physical security" or "life safety" security unless otherwise clarified.

Key Recommendations
The Master Security Plan identifies six key goals that can enhance security at UNC Greensboro.

- Goal #1: Centrally manage security risk
- Goal #2: Enhance security awareness through community engagement and education
- Goal #3: Integrate security into planning, design, construction, and facilities operations
- Goal #4: Implement measures to protect building perimeters
- Goal #5: Enhance security of campus perimeter and outdoor spaces
- Goal #6: Enhance security of campus communications and infrastructure

The Master Security Plan – based on quantitative data, risk assessments, and extensive interviews with members of the University community – provides a comprehensive roadmap for UNC Greensboro to further its security initiatives.

Introduction

The University seeks to be a leader among higher education institutions in proactively identifying, responding to, and mitigating security concerns. As a state-funded university, the UNC Greensboro campus was designed to be open to the public and the surrounding community. Historically, security has not been a predominant force or guiding principle in regard to site layout, building construction, maintenance, or operations. While UNC Greensboro is committed to maintaining an open and accessible campus environment for students, faculty, employees, and visitors, the University is equally committed to creating a safe and secure environment based on well-designed policies, procedures, and a robust security infrastructure.

The 2017-2020 Master Security Plan is designed to assist UNC Greensboro in creating a pathway forward to allocate resources in support of security programs and infrastructure. The plan recognizes the impact that a safe and secure academic setting has on the learning process and on the well-being of those who work, study, and visit the campus. It includes security guidelines and standards that will strengthen security within the university's existing infrastructure, facilitate a rapid response to emerging threats, and accommodate plans for continued growth and development across the campus.

The Plan is divided into three sections:

- **Security at UNC Greensboro Today** examines events that have shaped the University's security program.
- The **Strategic Plan** presents the goals and strategies to achieve the vision.
- The **Implementation Plan** provides an estimated timeline and budget to achieve key elements of the strategic plan.

This Master Security Plan is a living document. As such, it allows flexibility in its application for evolving risk and ongoing campus-wide planning initiatives.

Assessment Process

One of the key issues facing all university security programs is that national standards and national centers of excellence do not yet exist to provide clear direction for universities on policies, procedures, and best practices. Several tenets of physical security have emerged in government sector guidelines. Specifically, guidelines have been published by the Department of Homeland Security's Interagency Security Committee Standards and Best Practices, Department of Defense, FEMA, U.S. Department of Justice, Veterans Affairs, and the Smithsonian Institution. However, these documents do not provide adequate guidance on issues such as organizational structure, staffing, budgets, emerging technologies, metrics, benchmarking requirements, and more. This has forced all universities to independently develop security programs, drawing upon broader industry best practices for policing and physical security.

The University engaged internal groups and committees to conduct a quantitative security assessment and develop the Master Security Plan. We used multiple tools and processes to assess the current state of security on the UNC Greensboro campus, including the following:

- Interviews: Conducted meetings with University leaders, faculty, students, and staff
- Data analysis: Analyzed historical data, including crime statistics, calls for service, and response times
- Operational analysis: Analyzed existing security policies, plans, procedures, and operations
- Risk assessment: Conducted a detailed site survey and analysis of various facilities on campus

In recent years, UNC Greensboro has also conducted self evaluations, risk assessments, and initiatives focused on the physical security of the campus. While these efforts have helped to create a more secure campus, the findings have not been integrated into a comprehensive plan. To achieve an effective and comprehensive strategy, a prioritized, university-wide plan is needed.

Scope

The Master Security Plan provides a strategic management tool to guide UNC Greensboro over the next four years as it continues to maintain and improve the safety and security of the University.

The Plan focuses exclusively on the personal safety and physical security of people and property at UNC Greensboro. Physical security measures are aimed to prevent, deter, or inhibit crime and threats on campus. They are also designed to reduce any potential damage or injuries and to ensure a swift response should an incident occur. A well-constructed master security plan enables the University to meet new legislative requirements, limit exposure to liability, adapt to changing levels of risk, and promote a sense of well-being among the campus population.

The Master Security Plan provides clear strategic, operational, and resource management directives for managing security risks and offers recommendations that will allow the University's existing security program to become more effective and progressive. The Plan will be used as a foundation for the inclusion of design standards used for renovation and new construction of existing and new facilities.

Security at UNC Greensboro Today

Departments Responsible for Providing Security

The primary departments responsible for providing security services at UNC Greensboro are the University Police, Information Technology Services (ITS), the SpartanCard Center, Housing & Residence Life, Facilities Operations, and Design & Construction.

University Police Department
The University Police Department is a full-service agency that provides professional law enforcement, emergency response, crime prevention, community outreach, oversight of security officers and student rangers. It is made up of 37 sworn police officers and 19 civilians. The department is a fully accredited law enforcement agency through the Commission on Accreditation for Law Enforcement Agencies (CALEA). The department is comprises of five divisions:

- The Patrol Division is responsible for providing uniformed police services, emergency response, and community involvement.
- The Support Services & Community Relations Division is responsible for investigations, training, special events planning, victim assistance, crime prevention, threat assessments, and dignitary protection.
- The Emergency Management & Communications Division is responsible for emergency coordination, business continuity, police communications, and proprietary alarm monitoring.
- The Police Administration & Professional Standards Division is responsible for personnel, recruiting, policy management, strategic direction, regulatory compliance, and accreditation.
- The Technical Services Division consults, designs, integrates, and maintains the use of electronic security technologies and safety applications deployed on campus.

Emergency Management
The UNC Greensboro Office of Emergency Management is responsible for developing, implementing, and maintaining an institution-wide emergency management program that performs duties within the five mission areas of emergency management (prevention, protection, mitigation, response, and recovery) to provide for the safety and well-being of all university stakeholders. This includes comprehensive planning, training, and exercise programs that enhance UNC Greensboro's capabilities to manage large-scale incidents and disasters. Working in partnership with local, state, federal and private entities, the Office of Emergency Management works to provide an integrated emergency management program that will aid in supporting intellectual growth, service to the community and institutional research.

It is the goal of the Office of Emergency of Management to:

- Create a culture of preparedness among faculty, staff and students;
- Build a disaster resilient community starting from the individual up to the University;
- Mitigate against recognized hazards;
- Provide emergency preparedness training to faculty, staff and students;
- Ensure timely warnings of emergencies impacting the immediate health and safety of the campus-wide community;
- Ensure plans and resources are in place to effectively respond to emergencies and disasters on campus;
- Ensure that the University can continue critical operations during and after an emergency or disaster

- Develop a framework that will allow for a fast, efficient disaster recovery process following an emergency or disaster;
- Provide direct support to departments and individuals on emergency planning, coordination, and information management.

Information Technology Services

Information Technology Services (ITS) is UNC Greensboro's central technology organization, providing computing, communications, and data services, and consulting with students, faculty, staff, and affiliates on technology. ITS is responsible for planning and management of the transmission and utilization of data, voice, and video, in support of the university's academic and administrative goals. ITS promotes best practices, efficient procurement, and overall cost-effectiveness in the use of IT resources across the entire University.

ITS operates as a single department, with all budget and staff centrally managed. ITS includes the following work groups:

- Administrative Systems provides services integral to the delivery of effective, efficient, and reliable core business information systems. Primary responsibilities include: Analysis of university client information system requirements and recommendation of best practice solutions, installation and maintenance of vendor-supplied and locally developed systems, and providing services and solutions that enhance the value of university data in support of informed tactical and strategic decision making.
- Learning Technology and Client Services is committed to delivering responsive, high-quality, customer-oriented services and support that fosters a productive and stable instructional, research and administrative operational environment for the students, faculty, and staff. Services include: Maintenance and support of technology-equipped learning spaces, open-access computer labs and "TeleLearning" facilities, reliable internal and external ITS communication services, including web/mobile application development and support, and participation in campus-wide initiatives to assess and meet University information technology needs and support services.
- Systems and Networks is responsible for managing the end-to-end service delivery and support processes to ensure that agreed upon customer requirements and expectations are met at all times. Services include: Plan, design, and implement stable and secure IT voice and data network infrastructure, provide centrally hosted/managed enterprise services (file, Web, print, database, and application), provide hosting services for departmental servers, and provide real time monitoring and maintenance of ITS infrastructure.

SpartanCard Center

The SpartanCard Center manages physical University identities. This includes capturing and making photos accessible to appropriate stakeholders, acting as the gatekeeper to physical building access via UNC Greensboro’s new electronic door access system and performing database management to ensure separated individuals cannot enter University buildings using their ID card.

Housing & Residence Life

Housing and Residence Life (HRL) provides housing for over 5500 residential students and 5000 summer conference guests throughout the year. HRL facilities include student residences, multi purpose spaces for University functions as well as academic classrooms. Access into residence halls are managed by a combination of automated uploads based on housing assignment and manually assigned access by HRL staff. A decentralized management of access is utilized due to a constant fluctuation for access needs from students, faculty, staff, and vendors. Unlike administrative and academic buildings, HRL's default state for all perimeter access is locked. Alternate states can be requested by faculty or staff. Installation and maintenance is provided by HRL staff with after hours on-call support.

HRL also maintains cameras at entrances or high traffic areas. Cameras are accessible by UNC Greensboro Police and are positioned based on their recommendation. New camera locations are being added based on budget and renovations of existing buildings. All new buildings have camera facilities added in the building specifications.

Facilities Operations

The mission of Facilities Operations is to be a service organization comprised of skilled professionals dedicated to the continuous maintenance, operation, and improvement of University facilities and grounds, in order to provide a safe, clean and well functioning environment for all members of the University community. The Lock Shop falls under the direction of the Facilities Operations and consists of three locksmith technicians who perform a variety of services related to maintaining the mechanical security door hardware and keying needs of the university. These services include installation and service of keyed locks, controlling the master key system, and rekeying as needed. The Lock Shop logs all keys issued and maintains the electronic access systems in academic and administrative buildings.

Environmental Health and Safety

Environmental Health and Safety is a service-oriented organization dedicated to support the University's overall mission by inspiring a cultural environment of shared responsibility. This is accomplished by providing support services that include, but not limited to, education, resources, special services, oversight, and guidance in the following areas:

- Radiation Safety
- Fire and Life Safety
- Biological Safety
- Chemical and Laboratory Safety
- Occupational Safety
- Hazardous Waste Management
- Environmental Compliance

Fire and life safety falls under the direction of Environmental Health and Safety and consists of duties including the University Fire Marshal. Fire and life safety is responsible for code and regulatory oversight related to university buildings and rooms. These responsibilities include maximum occupancy and use classifications, entry and egress requirements and fire alarm system impairment procedures.

Design & Construction

Facilities Design & Construction (FDC) manages improvement projects through the design and construction phases for the University. FDC's mission is to minimize financial risk and achieve the best possible results within the budget and time frame required for the benefit of the entire campus community. The department builds consensus and educates faculty, staff, students, designers and contractors in order to achieve the highest quality product possible.

Security Challenges on Campus

One constant on every university campus is change. New students and faculty arrive on campus each semester. New employees are hired. New buildings are constructed, and existing buildings are renovated. New technologies are integrated into the campus environment. Special events require additional levels of security and protection. While this growth and development is a boon for the campus community, it can also create challenges for security.

The past decade has also brought about many changes in the public's perception of school safety and security, generating pressure for schools to examine their existing security systems and stay competitive and current in the marketplace. These changes to policies and procedures require planning and deep integration with the processes of growth and development over time at the university.

In order to provide context for the recommendations in this report, we have identified four key areas of growth and change on the campus that directly impact safety and security issues. These include (but are not limited to):

- New legislative requirements
- New and emerging technologies
- Dynamic and growing population
- New construction and renovation

New Legislative Requirements

The increase in high-profile incidents on U.S. campuses, particularly the tragedy at Virginia Tech and others, has pushed the issue of campus security to the forefront of the national consciousness. This in turn has led to several new federal policies, programs, and guidelines designed to regulate and monitor campus security. These new legislative requirements have demanded the attention of the university's security team at a time when they are already stretched thin.

These new requirements have wide-ranging and profound effects on the entire UNC Greensboro community, not just security personnel. The legislation requires close coordination among multiple programs and offices, data collection, diligent reporting of incidents, adoption of new policies and procedures, training mandates, and upgrades to existing systems and infrastructure. These mandates are all critical to uphold the highest level of safety on campus, but with these new requirements come additional demands on security personnel and resources. As a result of these legislative changes, a centralized organization would best coordinate and manage security operations and resources.

New and Emerging Technologies

Every year, the university expands the use of technologies designed to keep the campus safer and more secure. These include:

- Emergency Phones (i.e., Blue Towers, Areas of Rescue, Elevators, and Wall Mounted phones)
- Mass Notification & Mobile Safety Apps (i.e., BB Connect, LiveSafe, WEBS, and Flat Panels)
- Access Control & Perimeter Security Monitoring (e.g., Blackboard Transact and Parking Gates)
- Video Surveillance (e.g., Cameras and Automated License Plate Readers)
- Fire & Security Alarm System (e.g,. Contact ID, Standardization, and Network Transmission)
- Public Safety Radio & Cellular Connectivity (e.g., Bi-Directional Antenna/Digital Antenna System)
- Data and Telephonic Connectivity (e.g., VoIP, Wireless, and Citrix)
- Compliance & Accreditation (e.g., Clery, Title IX, and OSHA)

The installation of new electronic devices requires an up-front investment as well as recurring costs for training, operations, maintenance, and upgrades. These evolving security technologies also require increased levels of technical aptitude and training to be successfully deployed and maintained. More importantly, the electronic security system is most effective when consistent and dependable, a goal that requires a significant commitment of resources that we currently do not have.

Furthermore, the array of security devices across campus has become increasingly complex. To manage these new and emerging technologies, the security program needs a stable, sustainable, and scalable financial model for maintenance and operations.

Consumer-grade Internet of Things (IoT) devices such as cameras and doorbells will experience growth in the coming years. University students, faculty, and staff will have an expectation that devices designed and meant for the home can be installed and used at the office. Many of these devices have the appearance of providing physical security but they do not meet the level of functionality required for use within a University environment. In addition, these devices are generally incompatible with enterprise networking standards and can often pose a larger network security risk to the organization.

Dynamic and Growing Population

Every year, thousands of new students arrive on UNC Greensboro's campus. For many students, their college experience represents the first time they have ever lived on their own. Becoming security aware is a key part of this educational experience. Security awareness is also important for new hires, particularly employees responsible for closing down offices or laboratories at the end of the day. Faculty must be educated on a variety of policies, including lab safety, workplace violence prevention, sexual harassment, and federal compliance. In addition, the population at UNC Greensboro has grown in response to increased enrollment. In the Fall of 2014, UNC Greensboro's enrollment was 18,647 students. In the Fall of 2015, student enrollment was 19,393. The target enrollment for UNC Greensboro is 20,000 by 2018. From 1993 to 2016 the amount of area under roof grew from approximately 3,008,401 square feet to 6,509,252 square feet.

New Construction and Renovation

UNC Greensboro has grown significantly in recent years, particularly with the development of the Spartan Village and the new Kaplan Wellness Center. This rapid growth, while positive for the University as a whole, can create an uneven level of security across multiple facilities. A similar issue arises with renovations of older buildings, as the process of retrofitting older facilities with newer security features can be problematic. The process of design, construction, and renovation represents an ideal opportunity to build in effective security measures.

While the University's construction guidelines provide uniform and relevant information to designers on minimum construction standards required for University work, they have only recently included minimum security requirements. In addition, security decisions and funding for each facility are handled at the department or college level, not through a central organization responsible for campus-wide physical security. The safety and security of people and property on campus must be viewed as a University responsibility, not an individual department or unit responsibility. To achieve a solid baseline of security standards across all facilities at the university, the Master Security Plan recommends that security be integrated into all planning, design, construction, and facilities operations. The proposed "Safety and Security Steering Committee" structure provides for a centralized collection and prioritization of safety issues.

Furthermore, a large portion of the current and future development for UNC Greensboro, particularly the off-campus locations, are not supported by UNC Greensboro security staff. The Gateway University Research Park campuses and the Union Square campus offer research and development partners unparalleled access and proximity to students and researchers. Piney Lake and Three College Observatory are additional examples of off-campus locations that create unaddressed security liabilities.

Strategic Plan

UNC Greensboro is a vibrant educational institution, with more than 89 buildings on campus and 3 satellite campuses and leased space in 9 off-campus locations. As a large, urban, land-grant university, the security of the entire community is a top priority. The security challenges associated with the University's growth and change (described in the previous section of this report) require a comprehensive and consistent strategy. The Master Security Plan is designed to address these challenges in a cohesive and proactive manner.

The Strategic Plan is built upon two foundational principles: 1) multiple layers of security and 2) crime prevention through environmental design. These guiding principles provide an important complement to our physical security, as they ensure that security concerns are part and parcel of all decisions related to future growth and development.

Guiding Principles

The Master Security Plan implements a risk-based methodology to security planning which identifies existing or emerging vulnerabilities and provides strategies to address these issues. This approach enables university leaders to have better visibility into the overall security landscape and its strengths and weaknesses so that limited security resources can be allocated appropriately.

The goals outlined in this report should be addressed congruently. However, budgetary constraints may require a graduated approach to risk mitigation, and as such the goals and strategies have been prioritized based on criticality.

While some of these initiatives are already in progress, this document brings together all the components of an effective security program into a single, comprehensive plan. The goals and strategies outlined herein ensure that best practices for security are treated as a strategic imperative, whether in training new employees, constructing new buildings, or managing special events.

By implementing the strategies in this report, the university can:

- Ensure consistent application of security throughout the entire campus
- Develop increased security awareness within the UNC Greensboro community
- Establish sustainable and scalable security measures

Underlying Methodologies

Multiple Layers of Security

A strategic plan for security must address a wide range of critical issues, beginning with personal safety and extending outward to protect equipment, facilities, and the perimeter areas of campus. The Master Security Plan offers a multilayered approach to physical security. These layers, or concentric rings, show how multiple strategies must work together to create a safe and secure environment on campus. The strategic plan considers the whole environment—people, places, policies/procedures, and equipment—ultimately providing a comprehensive view of university security. The goal is to promote a campus culture where the sense of personal safety and security enhances the educational experience, promotes the success of students, and fosters a sense of well-being among staff and visitors.

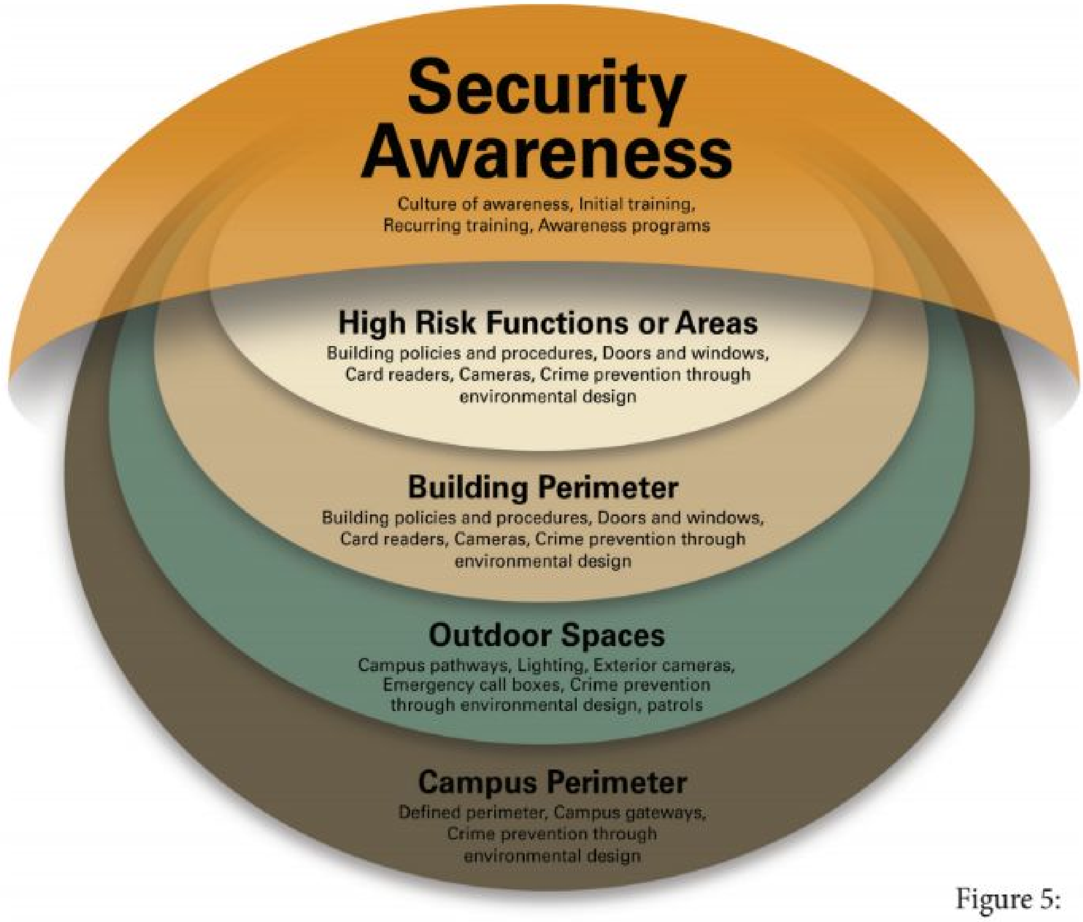

Security Awareness
Culture of awareness, Initial training, Recurring training, Awareness programs
High Risk Functions or Areas
Building policies and procedures, Doors and windows, Card readers, Cameras, Crime prevention through environmental design
Building Perimeter
Building policies and procedures, Doors and windows, Card readers, Cameras, Crime prevention through environmental design
Outdoor Spaces
Campus pathways, Lighting, Exterior cameras, Emergency call boxes, Crime prevention through environmental design, patrols
Campus Perimeter
Defined perimeter, Campus gateways, Crime prevention through environmental design

Figure 5: Multiple Layers of Security

Crime Prevention through Environmental Design

The Strategic Plan is also guided by the principles of crime prevention through environmental design (CPTED). Research into criminal behavior has demonstrated that thoughtful design of buildings, landscapes, and open spaces can reduce crime and create a safer environment. CPTED theory is based on four core strategies:

- Natural access control: Design entrances, lobbies, space adjacencies, exits, fencing, landscaping, etc. to clearly differentiate public vs. private space
- Natural surveillance: Place windows, restrooms, gathering areas, lighting, fencing, etc. to enhance the perception that people can be seen
- Territoriality: Use building layouts, interior design, signs, lighting, and landscape to express ownership
- Maintenance: Demonstrate ownership of the property through upkeep and a sense of order

When these CPTED principles are integrated into campus planning initiatives, they deter crime and promote a campus environment where students, faculty, and visitors can feel safer and more secure. CPTED underpins many of the goals outlined in the Strategic Plan.

Overview of Goals

The Master Security Plan recommends six goals to enhance safety and security on the UNC Greensboro campus. Each goal is supported by multiple strategies that can be put in place to achieve these goals. The Strategic Plan is based on findings from interviews, data analysis, and risk assessment.

Goal 1: Centrally Manage Security Risk

- Strategy 1.1 | Centralize the Responsibility for the Security Program
- Strategy 1.2 | Strengthen Existing Electronic Security System
- Strategy 1.3 | Implement Risk Management Process/Program
- Strategy 1.4 | Evaluate Current Funding for Security and Develop a Scalable Financial Model for the Future

Goal 2: Enhance Security Awareness Through Community Engagement and Education

- Strategy 2.1 | Assign Responsibility for the Safety and Security Awareness Program to the Community Relations Unit within the Police Department
- Strategy 2.2 | Develop Initial & Recurring Safety and Security Training and Awareness Programs
- Strategy 2.3 | Increase Visibility of Security on Campus
- Strategy 2.4 | Engage the Community

Goal 3: Integrate Security into Planning, Design, Construction, and Facilities Operations

- Strategy 3.1 | Develop Minimum Security Criteria
- Strategy 3.2 | Assimilate Security into the Planning Process
- Strategy 3.3 | Incorporate Security into the Design Process
- Strategy 3.4 | Integrate Security into the Construction Process
- Strategy 3.5 | Incorporate Security into Facilities Operations
- Strategy 3.6 | Implement Security Program for Special Events and Risk Mitigation

Goal 4: Implement Measures to Protect Buildings and Building Perimeters

- Strategy 4.1 | Implement Building Security Standard Operating Procedures
- Strategy 4.2 | Enhance Building Security with Mechanical Locks and Access Control
- Strategy 4.3 | Expand Campus Wide Video Surveillance System
- Strategy 4.4 | Actively Monitor Electronic Security Systems
- Strategy 4.5 | Maintain Reliability of Fire and Security Alarm Systems
- Strategy 4.6 | Develop and Sustain Automated External Defibrillator Program

Goal 5: Enhance Security of Campus Perimeter and Outdoor Spaces

- Strategy 5.1 | Define Campus Perimeter
- Strategy 5.2 | Develop Campus Gateways
- Strategy 5.3 | Clearly Delineate All Campus Pathways
- Strategy 5.4 | Create Uniform Lighting Standard
- Strategy 5.5 | Consistently Apply Security Technologies in Exterior Spaces

Goal 6: Enhance Security of Campus Communications and Infrastructure

- Strategy 6.1 | Evaluate the Effectiveness of the Mass Notification System & Other Methods
- Strategy 6.2 | Evaluate the Current Radio Receptions in All Facilities
- Strategy 6.3 | Evaluate the Current Cellular Reception on Campus
- Strategy 6.4 | Provide Stable, Well-Performing Core Enterprise Technology Services

Goal 1: Centrally Manage Security Risk

Centralized risk management enables universities to enforce clear and consistent security guidelines across all units on campus. The University does not currently have a centralized funding mechanism in place to support physical security across campus. Currently, individual UNC Greensboro units are responsible for managing and funding their own security decisions, which has led to an inconsistent level of security. Current funding for the security program is largely derived from 1) infrastructure assessment charges on security equipment being installed on new construction and renovation projects, 2) departmentally funded projects based on availability of discretionary funds, and 3) voluntary maintenance contracts applied to deployed equipment. Therefore, the current funding for security is volatile, as it is tied directly to project volume and discretionary departmental funding. By defining security as a university-level responsibility and establishing scalable funding formulas, UNC Greensboro can become more responsive to the changing risk environment and maintain a consistent level of security across all university units.

In 2009, the Police Department began collecting and allocating funds for security alarm monitoring and the campus enterprise camera system. These dollars were designed to help recover some of the infrastructure costs associated with maintaining the servers and licenses of these systems. However, it did not take into consideration any other expenses or personnel cost. Nor did it include any other security applications or technology based systems. In an effort to compensate, the police department created a Technical Services Division (TSD) to oversees all security based applications and technologies of the entire campus. TSD currently operates out of the Support Services Division with only one Technical Specialist. The unit is grossly understaffed and the demand for this type of technical support is never ending and rapidly increasing. This plan calls for the expansion of the Technical Services Division. TSD would be responsible for the consultation, design, integration, and maintenance of all electronic security technologies and safety applications. Although it would require additional staffing and funding to establish this resources, the University would have a consistent and appropriate response to the security application and technical needs of the entire campus.

Strategy 1.1 | Centralize the Responsibility for the Security Program

Establish the Safety and Security Subcommittee to serve as the de facto authority having jurisdiction of the security program. This will provide the subcommittee with the authority to define and implement consistent security measures across the university. Security recommendations made by the Safety and Security Subcommittee based on campus security standards and best practices should receive priority funding for implementation. By charging the subcommittee with the authority to establish standards – as opposed to making recommendations that can be accepted or rejected – the University can ensure a more uniform application of security measures as a whole.

Strategy 1.2 | Strengthen Existing Electronic Security System

As the University's technology infrastructure has grown, the demands on security personnel have grown along with it. In the past, the University has employed field technicians to manage its infrastructure of relatively straightforward security devices. As the number of servers has skyrocketed and the security infrastructure has evolved into complex Enterprise IT systems, the cost of labor and the number of highly skilled IT professionals needed to support these complex systems has increased significantly. There is an immediate need for additional full-time system analyst and field technicians to support system growth. In addition, the burgeoning server infrastructure and remote administration of keys also require dedicated resources.

Strategy 1.3 | Implement Risk Management Process/Program

Implement a risk assessment program that will allow the university to consistently and effectively manage risk. To achieve this goal, the University should take the following actions:

- Use the risk registry tool to conduct an initial assessment of each facility. The tool identifies high-risk facilities and easily compares security levels among similar buildings, enabling prioritized allocation of resources. It provides a baseline that enables administrators to monitor changes in security risk and threats over time.
- Allocate resources based on findings from the risk assessment, prioritizing security measures for high-risk facilities and areas before those with lower associated risks.
- Conduct regular risk assessments to 1) identify changes in assets and threats, 2) evaluate the effectiveness of the security measures implemented since the prior assessment, 3) identify additional security measures required, and 4) prioritize these efforts across the university.
- Reduce the expanding administrative burden of sworn police officers by hiring a full-time (non-sworn) administrative employee to handle responsibilities Clery compliance and allowing sworn officers to focus on traditional policing duties.
- Implement a risk management process based on the Plan-Do-Check-Adjust (PDCA) approach. Used in ANSI standards, PDCA is a four-step management method that provides a structure for a security program to continually improve and adjust to a changing environment. See Figure 7 for a risk management process using PDCA that could help UNC Greensboro move forward on the Master Security Plan.

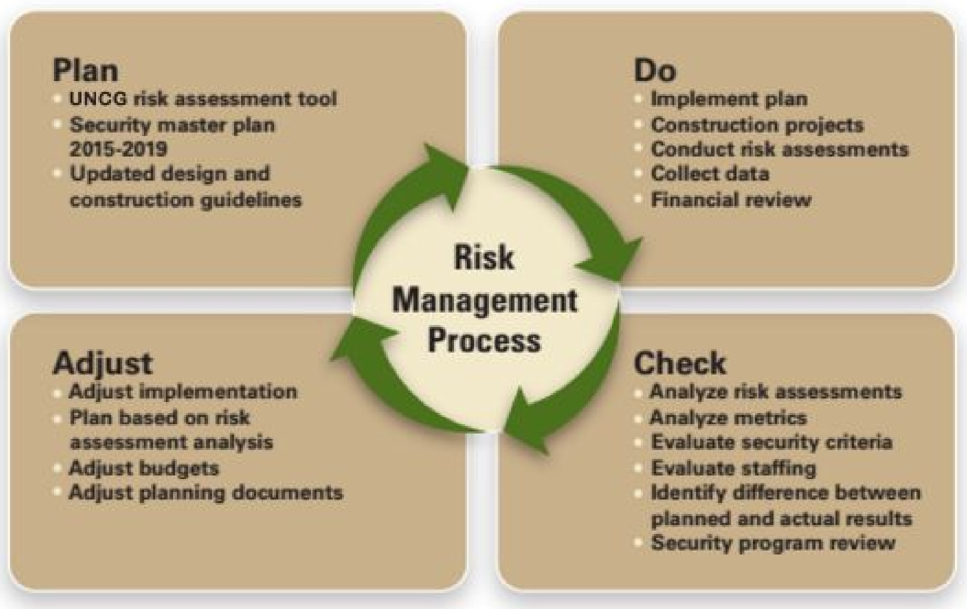


Figure 7: Risk Management Process

This kind of careful process can prevent wasting valuable resources on unnecessary protection or failing to provide adequate protection at crucial areas.

Strategy 1.4 | Evaluate Current Funding for Security and Develop a Scalable Financial Model for the Future

While this Plan addresses existing and near-term security needs, the University requires a comprehensive and scalable funding solution for security that can be sustained over the long term. As the University continues to grow and evolve, funding formulas for the security program must scale in response to this growth. Security must also be viewed as a University-level responsibility. As such, the University should conduct a thorough financial evaluation of the entire security program to identify which assets have the greatest demand for security (prioritizing assets with increased liability) and determine which metrics should be tracked. Once complete, this evaluation will yield scalable formulas for determining security funding allocations.

Financing the Master Security Plan will be challenging in an atmosphere of budget austerity and competing demands for limited dollars. Currently, security operating expenses are incorporated into UNC Greensboro's operating budget without a clearly defined source of financing. To remedy this situation, the financing plan will likely need to include a variety of revenue sources. Considering the vast array of security systems and security users on campus, it is likely that the source of funding will need to come from a multitude of users and facilities. Approaching the financing plan in this way will promote an equitable and affordable solution.

Funding possibilities could include the following sources of revenue:

- Reversion and Carry Forward
- Repair and Renovation funds
- Appropriated dollars for capital projects
- New user fees from campus units, specifically for security
- Expansion or redefinition of existing student fees
- Maintenance and operations funding and/or an expansion in administrative facilities fees

Goal 2: Enhance Security Awareness Through Community Engagement and Education

The University population is transient and as such requires frequent formal and informal security awareness training. The goal is to educate students, faculty, and staff so they know how and when to report an incident if it occurs, and what measures can be taken to prevent incidents from occurring. While it is beyond the power of the University to completely insulate the campus community from the threats that exist in our society, security awareness training can empower individuals to take responsibility for their safety and security on campus (see Figure 8).

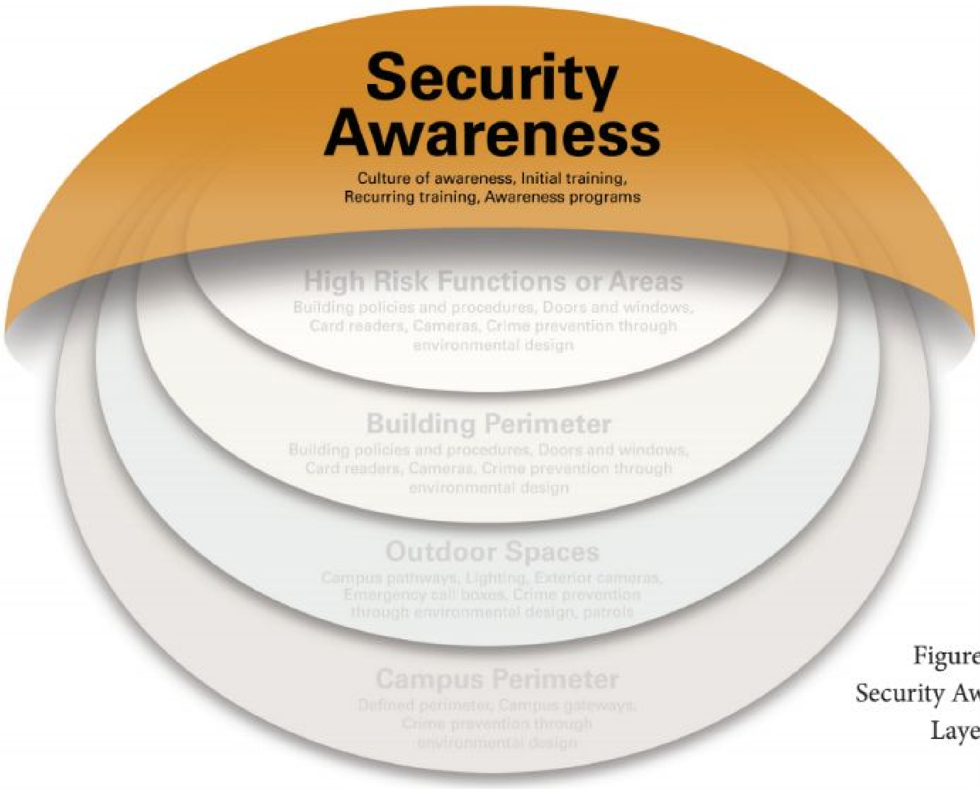

Security Awareness
Culture of awareness, Initial training, Recurring training, Awareness programs
High Risk Functions or Areas
Building policies and procedures, Doors and windows, Card readers, Cameras, Crime prevention through environmental design
Building Perimeter
Building policies and procedures, Doors and windows, Card readers, Cameras, Crime prevention through environmental design
Outdoor Spaces
Campus pathways, Lighting, Exterior cameras, Emergency call boxes, Crime prevention through environmental design, patrols
Campus Perimeter
Defined perimeter, Campus gateways, Crime prevention through environmental design

Figure 8:
Security Awareness
Layer

UNC Greensboro offers several in-person training programs for students, faculty, staff, and new employees, based on nationally recognized best practices. While these training sessions are of great value to the campus community, the security program has limited resources, and they are not required nor audited. Enhanced safety and security programs can provide the knowledge to help keep people safe on and off campus.

Strategy 2.1 | Assign Responsibility for the Safety and Security Awareness Programs to the Community Relations Unit within the Police Department

Designate the Community Relations Unit within the Police Department as the responsible party to centralize the security awareness program. By creating a single point of contact for security training and community outreach, the university can ensure that a consistent level of safety and security awareness training is being implemented for all students, faculty, staff, and new employees.

Strategy 2.2 | Develop Initial and Recurring Safety and Security Awareness Programs for Students, Staff & Faculty

Create a series of mandatory safety and security awareness programs for all individuals affiliated with the university. Attendees will learn how to identify and manage personal risk on and off campus. This strategy includes both initial training and annually recurring training sessions. One method to achieve this may be to require students, faculty, and staff to complete online security awareness training courses as part of orientation or prior to being issued an ID card or authorized to register for classes.

In addition to creating new training, it is recommended that the University further develop its existing security awareness programs in concert with police department's community policing efforts. This will ensure a greater variety of content to keep the University's disparate populations more engaged. The University should provide its students, staff, and faculty with periodic reminders between annual training sessions to promote a continual state of awareness. Programs should be geared to address issues that arise for specific groups on campus, such as resident students vs. non-resident students, resident directors, resident assistants, faculty, staff, grounds maintenance crew, housekeeping, and contractors. Trainings can be conducted through a variety of means, including:

- Orientation Programs (SOAR, NEO, Middle College, and International Students)
- Online Training through Canvas and PowerDMS
- Partnerships with faculty, staff, and student organizations.
- Targeted In-Person Classes (e.g. Run Hide Fight, Clery Act & Title IX, etc.)

Training sessions could also cover important security topics, including walking the campus at night, reporting incidents, the SpartanCard, workplace violence, building access control, building closing procedures, active shooter, sheltering-in-place, use of emergency phones and the LiveSafe app and more.

Strategy 2.3 | Increase Visibility of Security on Campus

Security Officers provide a visible security presence on campus and an economical alternative for the department to address less critical duties. Increasing the number of uniformed security officers and rangers (student security officers) to help with the growth of the campus, overtime events, and lower priority calls.

- Conduct campus patrols and building checks
- Respond to verified non-emergency alarm events
- Respond to open door alarms
- Conduct door checks outside of normal business hours
- Testing emergency phones, cameras, panic buttons, and automatic external defibrillators.

Strategy 2.4 | Engage the Community

Trust between law enforcement agencies and the people they protect and serve is essential. It is key to the stability of our communities, the integrity of our criminal justice system, and the safe and effective delivery of policing services. In light of the recent events that have exposed rifts in the relationships between local police and the communities they protect and serve, on December 18, 2014, President Barack Obama signed Executive Order 13684 establishing the Task Force on 21st Century Policing. The President charged the task force with identifying best practices and offering recommendations on how policing practices can promote effective crime reduction while building public trust. The task force recommendations, each with action items, are organized around six main topic areas or "pillars:"

- Pillar One: Building Trust and Legitimacy - Building trust and nurturing legitimacy on both sides of the police/citizen divide is the foundational principle underlying the nature of relations between law enforcement agencies and the communities they serve. Decades of research support the premise that people are more likely to obey the law when they believe that those who are enforcing it have authority that is perceived as legitimate by those subject to the authority. The public confers legitimacy only on those whom they believe are acting in procedurally just ways.
- Pillar Two: Policy and Oversight - emphasizes that if police are to carry out their responsibilities according to established policies, those policies must reflect community values. Law enforcement agencies should collaborate with community members to develop policies and strategies for deploying resources that aim to reduce crime by improving relationships, increasing community engagement, and fostering cooperation.
- Pillar Three: Technology & Social Media - The use of technology can improve policing practices and build community trust and legitimacy, but its implementation must be built on a defined policy framework with its purposes and goals clearly stated.
- Pillar Four: Community Policing & Crime Reduction - focuses on the importance of community policing as a guiding philosophy for all stakeholders. Community policing emphasizes working with neighborhood residents to co-produce public safety. Law enforcement agencies should, therefore, work with community residents to identify problems and collaborate on implementing solutions that produce meaningful results for the community.
- Pillar Five: Training & Education - As our nation becomes more pluralistic and the scope of law enforcement's responsibilities expands, the need for expanded and more effective training has become critical. Today's line officers and leaders must be trained and capable to address a wide variety of challenges including international terrorism, evolving technologies, rising immigration, changing laws, new cultural mores, and a growing mental health crisis.
- Pillar Six: Officer Wellness & Safety - The wellness and safety of law enforcement officers is critical not only for the officers, their colleagues, and their agencies but also to public safety. Pillar six emphasizes the support and proper implementation of officer wellness and safety as a multi-partner effort.

The 21st Century Policing report contains 60 recommendations and 92 action items for law enforcement. The UNC Greensboro Police Department will continue working toward complying with the recommendations and action items of 21st Century Policing. Currently, we have completed or made substantial progress on all of these with only 24 items remaining.

Goal 3: Integrate Security into Planning, Design, Construction, and Facilities Operations

The process of growth and development on a university campus involves many activities and decisions that can take place over a long period of time. Teams in charge of planning, design, financing, construction, and operations make decisions that impact security. A collaborative, multidisciplinary approach to implementing security measures is an established, efficient, and affordable way to plan, design, build, and operate security for a facility that the university establish minimum levels of security to be integrated into every construction project, incorporate security guidance into the design guidelines, and include security as part of the design, construction, and operations for a facility. By instituting these baseline levels of security on a campus-wide basis, the university will ensure that appropriate security measures are well-integrated into new facilities on campus.

Strategy 3.1 | Develop Minimum Security Criteria

Revise the University Design and Construction Guidelines to establish minimum security criteria. Once revised, the security criteria should be considered mandatory and used to help ensure that security is applied consistently. The objective is to ensure that campus planning initiatives incorporate cost-effective security solutions that provide appropriate levels of protection for the facility.

The security criteria will be applicable to any facility on UNC Greensboro property, whether occupied or leased to others. The University is responsible for all activities it sponsors and for the safety and security of land lease or commercial lease facilities on UNC Greensboro property. These facilities should meet the same minimum security standards and operate on the same security systems.

Strategy 3.2 | Assimilate Security into the Planning Process

Establish physical security as a guiding principle of the FDC design guidelines, using crime prevention through environmental design principles and other best practices outlined in the Master Security Plan. When planning capital improvement projects, requirements should include those related to security. By considering security at this early stage, planners are better able to identify conflicts between security and other functions. Early integration of security into a project also supports the budgeting processes by addressing rough order of magnitude and long-term maintenance and operations (M&O) costs.

Strategy 3.3 | Incorporate Security into the Design Process

Incorporate security reviews into the design process for new buildings and outdoor spaces to ensure that security requirements are neither overlooked nor removed from the project as the design evolves. Security providers should collaborate with designers in the early stages of a project to assess a new site, evaluate its risks, and collaboratively develop design solutions.

Strategy 3.4 | Integrate Security into the Construction Process

Incorporate security reviews into the construction process. A security professional can oversee proper implementation of security requirements during construction and ensure that all means and methods of installation are in accordance with the design and construction documentation. Furthermore, as changes occur or issues present themselves, a security professional can ensure that the minimum security standards remain intact.

Strategy 3.5 | Incorporate Security into Facilities Operations

Update facility and grounds maintenance procedures with new security criteria (as identified in Strategy 3.1). The updated University Design and Construction Guidelines will affect facility and grounds maintenance plans and procedures for items such as landscaping, lighting, and door hardware.

Strategy 3.6 | Implement Security Program for Special Events and Risk Mitigation

Develop and implement a centralized security program to coordinate security and risk mitigation around upcoming events. The program will address how departments and organizations that are sponsoring events will identify, communicate, plan, and coordinate security requirements. This will address pre-event planning, management during the event, incident response, and post-event activities.

Goal 4: Implement Measures to Protect Higher-Risk Areas and Building Perimeters

Electronic security systems act as cost-efficient force multipliers, enhancing the capabilities of campus security. These technologies control building access, provide live camera feeds and forensic data of incidents, and alert security personnel to breaches. Electronic security has become the standard for university, government, and corporate facilities to protect building perimeters and high-risk areas.

In April 2013, executive staff at the University viewed and accepted a proposal for unified access control at UNC Greensboro. This established a roadmap to secure and monitor the perimeter of all University facilities, with the belief that this action is fundamental to personal safety and the physical security of the campus. Controlling access was recognized as our first line of defense against theft, intrusion and violent crime, while acting as a cost-efficient force multiplier for campus security staff. In addition, a GA Task Force recommended that construction and renovation budgets include the cost of procuring and installing building security systems, and that building operating budgets must provide for the ongoing operation of these systems.

As a result, Blackboard Transact, the University's existing ID card transaction system, was leveraged to include an access control component. As of Fall 2015, UNC Greensboro had converted 449 doors to this new system. This total included all Housing and Residence Life exterior doors and many academic and administrative buildings. The University will establish a baseline level of security at building perimeters and high-risk areas. Figure 10 demonstrates how this goal builds on the layers of security.

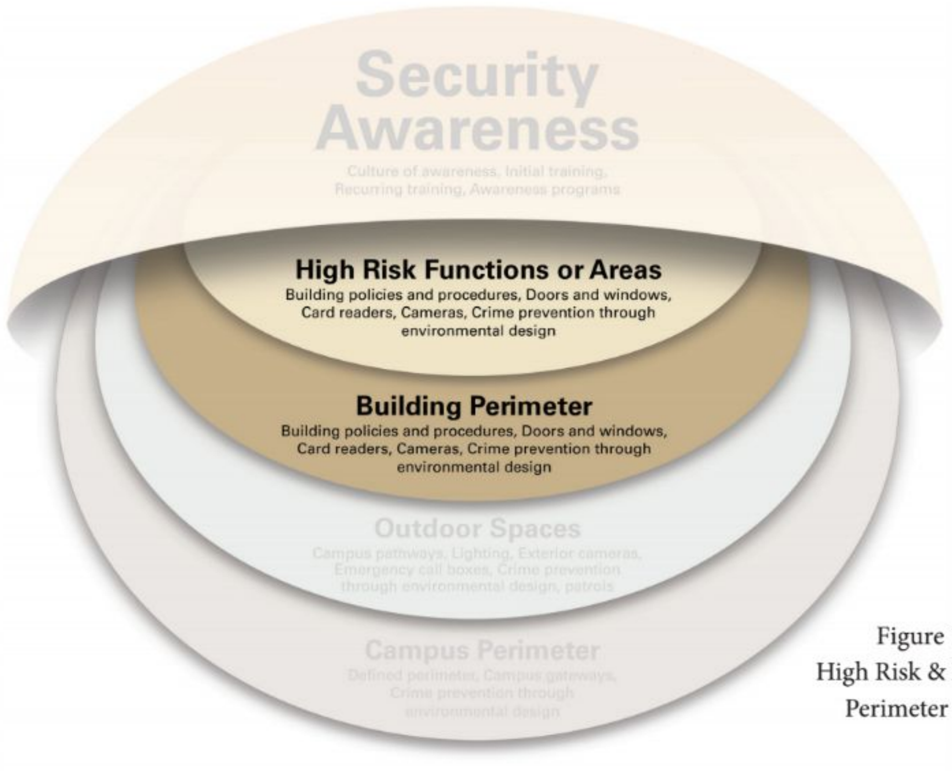

Security Awareness
Culture of awareness, Initial training, Recurring training, Awareness programs
High Risk Functions or Areas
Building policies and procedures, Doors and windows, Card readers, Cameras, Crime prevention through environmental design
Building Perimeter
Building policies and procedures, Doors and windows, Card readers, Cameras, Crime prevention through environmental design
Outdoor Spaces
Campus pathways, Lighting, Exterior cameras, Emergency call boxes, Crime prevention through environmental design, patrols
Campus Perimeter
Defined perimeter, Campus gateways, Crime prevention through environmental design

Figure 10:
High Risk & Building
Perimeter Layer

Strategy 4.1 | Implement Building Security Standard Operating Procedures

This strategy includes the development of building security standard operating procedures (SOPs) for each building and specific higher-risk areas. This effort ensures standard procedures for security operations across the whole campus. The most effective approach is to designate and compensate an individual in each building/department who is responsible and accountable for enforcing the procedures. This individual would be responsible for the following:

- Coordinate hours of operation and regular access needs with the Spartan Card
- Be the access control coordinator for the building; special events and reservations
- Conduct access audits to ensure the integrity of the access control system and accountability of keys for exterior doors
- Enforce the building's security operating procedures
- Manage the Emergency Action Planning process for the building/department
- Communicate with police and administrators about security concerns

Strategy 4.2 | Enhance Building Security with Mechanical Locks and Access Control

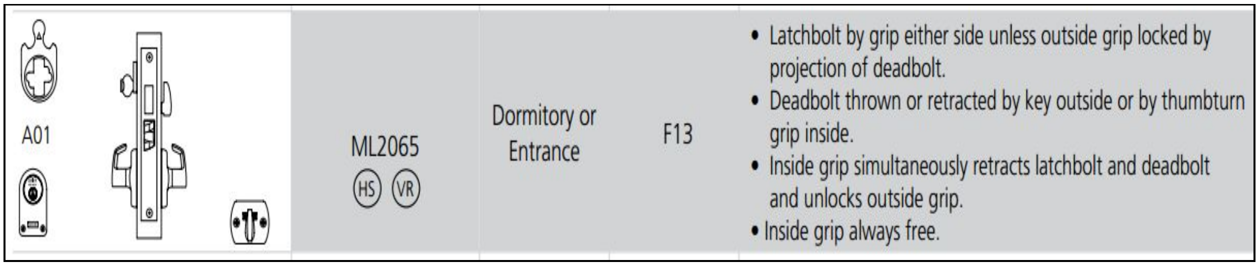
As part of the University's ongoing safety and security initiative, the Safety and Security Committee is recommending the installation of classroom locks on classroom doors with less than 50. The committee also recommends incorporating this requirement into the Facilities Design and Construction guidelines for all new construction projects.

The police department's "Run, Hide, Fight" program teaches that avoiding or escaping from an active shooter or violent situation is always the best option. However, when forced to hide, the campus community needs safe ways to do it. It is advisable for individuals to hide behind locked doors whenever possible. Active shooters typically do not take time to breach locked doors. Hiding behind an unlocked door can result in the least desirable and final option: fighting for your life with an armed assailant. Barricading a door that does not lock can be very difficult and, in some cases, impossible. Providing the means to safely shelter-in-place (taking immediate shelter in an accessible location), while help is on the way, can save lives.

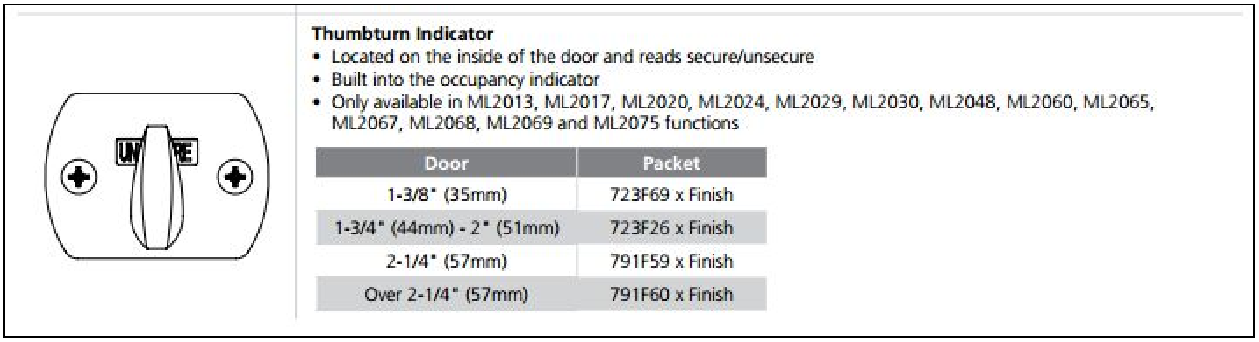
The overall increase in attacks and threats of mass violence have caused us to reevaluate the associated risks. The committee recognizes the inherent strategic risk associated with having locks on classroom doors but believes that the safety benefits outweigh the potential risk.

While there are many types of locks and lock functions available for use on classrooms, each has its own set of benefits and challenges. Mechanical locks have traditionally been the norm in classrooms. There are a number of "typical" functions used to secure doors that are unique to the overall security needs of the facility. No one function is right for every door and we must consider the occupancy and function of each room as it changes from semester to semester.

Below is an illustration of the locks that have been recommended by Facilities.



A01	ML2065 HS VR	Dormitory or Entrance	F13	• Latchbolt by grip either side unless outside grip locked by projection of deadbolt. • Deadbolt thrown or retracted by key outside or by thumbturn grip inside. • Inside grip simultaneously retracts latchbolt and deadbolt and unlocks outside grip. • Inside grip always free.



Thumbturn Indicator

- Located on the inside of the door and reads secure/unsecure
- Built into the occupancy indicator
- Only available in ML2013, ML2017, ML2020, ML2024, ML2029, ML2030, ML2048, ML2060, ML2065, ML2067, ML2068, ML2069 and ML2075 functions

Door	Packet
1-3/8" (35mm)	723F69 x Finish
1-3/4" (44mm) - 2" (51mm)	723F26 x Finish
2-1/4" (57mm)	791F59 x Finish
Over 2-1/4" (57mm)	791F60 x Finish

Electronic access control systems (i.e., card readers) provide the following benefits over mechanical locks and keys: 1) digital management of access rights, allowing for fast deactivation of access rights, 2) capability to remotely lock down facilities, 3) aid to law enforcement in the event of an incident, 4) the ability to monitor door status, 5) provide audit trails for forensic investigation, and 6) reduce cost of rekeying if a key is lost. The University currently uses locks and keys for perimeter locking of the majority of its buildings. To increase building security, the University should adopt electronic access control systems and video cameras on perimeter entrances to all campus buildings.

The following actions are recommended:

- Designate and clearly identify building entrances and install card readers and electronic locking hardware
- Secure perimeter doors to mechanical, electrical, and other utilities with door position switches and keyed locks with limited distribution of the keys
- Upgrade the campus lock sets to match the new University standard
- Equip exit-only doors with door contacts, local sounders, and remote monitoring, remove any existing exterior door hardware
- Install classroom functioning locks that allow members of the University to safely shelter-in-place
- Continue to inventory and assess status of access control and surveillance cameras
- Replace existing Millennium door system
- Assess compliance with the University's Physical Access to Information Technology Resources policy; convert physical access controls to IT Secure Areas where applicable
- Revise Construction and Renovation Guidelines for access control and cameras
- Install video cameras at all building entrances and exits

Strategy 4.3 | Expand Campus Wide Video Surveillance System

Assessment of servers, cameras and their placement is needed to ensure a functional surveillance network. Replacement of aging servers and cameras will be needed to accommodate more efficient cameras and increased storage for longer retention times and for recording at higher resolutions. An annual refresh cycle is needed to guide stakeholders in budgeting and maintaining their camera systems.

- There are 709 total cameras on the campus video surveillance network; 58 of these cameras are currently out of service for a variety of reasons.
- Defining guidelines for placement and management of cameras will create useable camera footage for UNC Greensboro Police and stakeholders. Proper management will provide a better understanding of purchasing server systems and cameras. This effort can reduce the overall cost of camera systems, standardize equipment, and create a useable surveillance network.
- Any expansion or change to the existing video system should be vetted with ITS to ensure these changes do not adversely impact network performance. Use of high-definition cameras, high frame rates, and 24-hour recordings can increase the consumption of network bandwidth at an alarming rate, potentially making the UNC Greensboro network performance unacceptable for enterprise applications. UNC Greensboro seeks to balance frame rates and motion detection with storage and network bandwidth utilization to achieve its goals with respect to video surveillance.
- The stakeholder committee will be directed to understand the business needs within the University. The committee can standardize equipment and create guidelines for managing camera systems. The primary focus would be safety and security of UNC Greensboro's students, staff, faculty, visitors, and assets, with an emphasis given to perimeter security of campus and building entrances.
- Defining construction and renovation guidelines for incorporating cameras is vital to the future expansion of the surveillance network. Guidelines should include placement and pathways to the network infrastructure for interior and exterior cameras. Completing this work during construction and renovation provides an opportunity to reduce future costs and provide options for future expansion of the surveillance network.

Strategy 4.4 | Actively Monitor Electronic Security Systems

Fire officials verify that fire alarm systems central station are installed per applicable code requirements. However, once these systems are installed, it is a challenge for many jurisdictions to ensure they continue to comply with code requirements. The UL fire alarm certificate program is designed to make sure that systems will continue to be tested and maintained after their initial system acceptance, and at minimal cost to the jurisdiction (http://www.ul.com/code-authorities/).

- **Codes require central stations to be listed** - Fire codes require some fire alarm systems to be monitored by an approved supervising station in accordance with NFPA 72, and fire officials often require these systems to be monitored by a UL Listed facility which is consistent with NFPA 72. We are exempt from this requirement under our proprietary status but UL fire alarm certificate program embodies the best practices of prevention, detection, and response.
- **Full central station service includes more than just monitoring** - Central station service complying with NFPA 72 includes all of the following elements:
    - Proper installation of the alarm system
    - Alarm, supervisory, and trouble signals that are monitored and responded to in a timely fashion
    - Alarm signals that are retransmitted to local authorities with no delays
    - Alarm system record keeping and reporting
    - Periodic system testing and maintenance
    - Prompt runner (technician) dispatch
- **What is covered by a UL central station listing?** - UL performs an initial investigation to verify compliance with NFPA 72 and UL 827. Companies that demonstrate compliance obtain a central

station listing. UL also performs periodic audits of listed central station facilities to verify ongoing compliance. Some of the high points of the audit are as follows:

- The central station building continues to be properly constructed and secured
- Primary and standby power are provided, maintained and periodically tested
- Listed fire alarm receiving equipment and spare parts are provided
- Sufficient staff is on duty at all times to handle alarm signal receipt and required responses
- Records of all fire alarm activity are maintained for certificated alarm systems (a key distinction)

Strategy 4.5 | Maintain ***reliability*** of fire and security alarm systems for all facilities on campus

UNCG currently has building fire alarm systems of various ages. To maintain the reliability of these systems and to avoid false reporting due to unstable systems, a prioritized plan for system replacement needs to continue to be maintained and funding provided at an adequate level. Priority will be determined by system issues, system age, and ability to continue to obtain parts and service. New fire alarm systems shall include mass notification. New fire alarm systems will also need to have the appropriate level of oversight and checkout during installation to ensure that, upon acceptance, alarm information indicating type and location is accurate and false alarm reporting is avoided.

Strategy 4.6 | Develop and Sustain Automated External Defibrillator Program

UNC Greensboro is committed to the health and safety of its students, faculty, staff and visitors who are in and out of our buildings daily. Each year, sudden cardiac arrest (SCA) strikes more than 350,000 Americans. During SCA the victim immediately becomes unresponsive, stops breathing, has no pulse, and will die within minutes without intervention. The primary cause of sudden cardiac arrest is ventricular fibrillation, a condition in which the heart's normal electrical signal becomes erratic, causing the heart to cease pumping blood effectively. When this occurs, defibrillation, or restoring the heart's natural rhythm by applying an electrical shock, is the best treatment of SCA. The chance of survival decreases by approximately 10% with each minute that passes after the time of the attack. The response time by emergency medical services (EMS) personnel is often more than the nationally accepted ideal time for defibrillation following an episode of SCA, which is within two (2) minutes. Widespread deployment of automated external defibrillators (AED) allows community members to provide early defibrillation to victims in the first critical moments after a SCA. Use of an AED does not replace the care provided by EMS, but is meant to provide a lifesaving bridge during the first few critical minutes it takes for advanced life support providers to arrive.

In 2012, the North Carolina General Assembly codified North Carolina General Statute **§ 143B-370.1. Defibrillators in State buildings**, stating that all state buildings must implement a lay rescuer AED program, to include an AED maintenance program that ensures proper maintenance and testing of AED devices. Currently at UNC Greensboro there is no such AED program in existence.

To date, there are approximately 45 AEDs on campus, either in vehicles or mounted in buildings. These AEDs were purchased by departments over the past several years using departmental funds and come in a variety of makes and models. The larger departments possessing AEDs have some sort of training, maintenance, and testing processes; however, each varies in scope and complexity. Smaller departments that possess AEDs do not have processes in place to train staff and maintain their AED equipment. In addition to the lack of consistent training and maintenance processes for AEDs on campus, there is also a lack of uniformity in the type of AED purchased, how the AED is mounted and where, and who is responsible for training and maintenance processes.

To bring UNC Greensboro into compliance with NCGS § 143B-370.1; unify the purchase, placement, testing, maintenance, and training; and increase the availability of AEDs on campus, the University should:

- Establish a centralized AED program that is managed by one department
- Create a University-Wide AED Policy that establishes standards for the purchase, placement, use, testing, and maintenance of AEDs
- Establish an annual budget to sustain the AED program
- Create a lay rescuer AED training program
- Through a phased approach, place an AED in each building on campus, placing priority on high-risk buildings first**.**

Goal 5: Enhance Security of Campus Perimeter and Outdoor Spaces

An effective security program not only reduces risk, but it reduces the perception of risk. By creating an environment that allows students, faculty, staff, and visitors to feel safe and secure, the University can better achieve its educational mission. As a large, urban university, UNC Greensboro must differentiate the campus environment from its surrounding environment. Using the principles of crime prevention through environmental design, it is recommended that the University clearly delineate the campus perimeter. By using buildings, gates, signs, lighting, and landscape to reinforce campus boundaries, a sense of ownership exists on campus. In this sense, “strangers” or “intruders” tend to stand out, and the campus becomes a less attractive target for crime. As seen in Figure 11, this strategy continues to build on the layers of security.

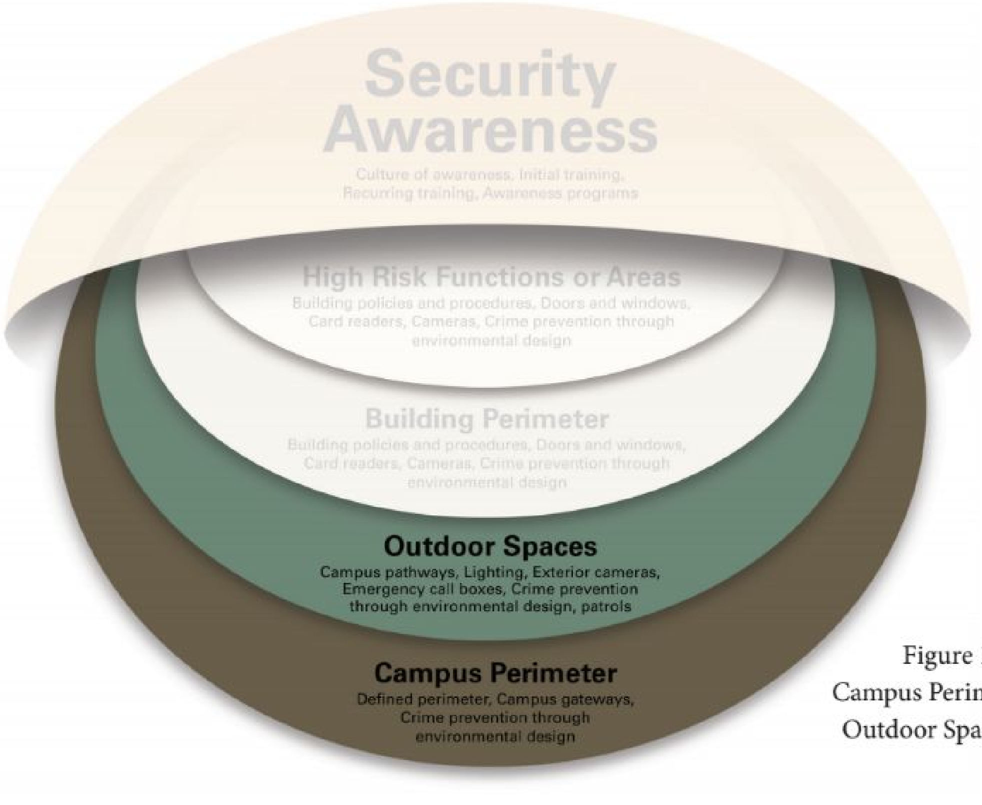

Security Awareness
Culture of awareness, Initial training, Recurring training, Awareness programs
High Risk Functions or Areas
Building policies and procedures, Doors and windows, Card readers, Cameras, Crime prevention through environmental design
Building Perimeter
Building policies and procedures, Doors and windows, Card readers, Cameras, Crime prevention through environmental design
Outdoor Spaces
Campus pathways, Lighting, Exterior cameras, Emergency call boxes, Crime prevention through environmental design, patrols
Campus Perimeter
Defined perimeter, Campus gateways, Crime prevention through environmental design

Figure 11:
Campus Perimeter and
Outdoor Space Layer

Strategy 5.1 | Define Campus Perimeter

Define the campus perimeter by providing clear visual indicators of where university property begins. This effort creates a sense of ownership, indicating that the university has an active interest in its boundaries. Use buildings, fences, pavement, signs, lighting, and landscape to define university space.

Strategy 5.2 | Develop Campus Gateways

Create additional gateways at vehicle and pedestrian entrances to support the delineation of the campus perimeter. Conversely, limit or reduce usage of low-traffic entrances to the greatest extent possible. Implementing these controls will funnel the majority of site users to defined entrances and exits, support wayfinding, and also enhance access control. This effort supports surveillance—both natural (visual) and video—by establishing key choke points from which to observe people entering and exiting campus.

Strategy 5.3 | Clearly Delineate All Campus Pathways

Develop pathways through campus that provide clear lines of sight. Use low-growing vegetation to line pathways and ensure that canopies are sufficiently high. This design provides an open, inviting environment in which users can see and be seen—both key aspects to feeling safe. This design also minimizes issues of vegetation blocking the light from fixtures illuminating the paths.

Strategy 5.4 | Create Uniform Lighting Standard

In conjunction with the Facility Master Plan, modify lighting across the University to meet the Guideline for Security Lighting by the Illuminating Engineering Society of North America. This may include additional lighting in areas, reduction of lighting in areas, planned transition lighting, and changes to some lamp types.

Strategy 5.5 | Consistently Apply Security Technologies in Exterior Spaces

Develop a strategy for the consistent application of security technologies in exterior spaces across campus. There are few exterior cameras and the existing emergency blue light phones were implemented prior to the wide availability of cellular telephones. Blue light phones are rarely used for emergency calls; instead, people access them to request non-emergency assistance (e.g., escorts). The University has established a pilot program to test a cellular solution in strategic locations. The cellular option may be more efficient than the existing landlines and reduce cost.

For several years, the police department has conducted an inventory and assessment of all the emergency phones on campus. This includes the blue tower phones and all interior and exterior wall mounted emergency phones, as well as all areas of rescue and elevator phones. Currently, there are 292 emergency phones on campus, comprised of: 114 blue tower, 35 interior wall mounted, 33 exterior wall mounted, 23 areas of rescue, and 87 elevators.

During our assessment, we discovered numerous problems with the emergency phones that ranged from being totally out of service to burned out light bulbs. A few of the major issues are:

- The phones are occasionally removed, added, or relocated without the police department’s knowledge.
- The phones in the parking decks were purchased from a different vendor and cannot be repaired by UNC Greensboro ITS Voice Services; the proprietary phones must be serviced by the vendor, Code Blue, which has been known to take several weeks to address.
- Several emergency phones share a common number with no way to identify the specific location of the caller, other than a generic location such as the “McIver Deck.”
- The most troubling issue we found with the emergency phones is that the issues are sporadic and the phones work intermittently. There are some blue tower phones with emergency and info buttons that work one minute and don’t the next. To make matters worse, some of these phones are located in secluded areas where they are needed the most.
- Many of the WEBS (Wide-area Emergency Broadcast System) and building mass notification announcements are inaudible due to static and poor sound quality.

We continue to coordinate our efforts with ITS to resolve these issues, but there are a considerable number of problems with the emergency phones and we spend close to $100,000 a year in line costs alone. The emergency phones are the least used form of communications on campus. Out of the 9,318 calls made to Police Communications in 2014, there were only 80 calls received from emergency phones. The following year it was even less with only 78 out of 9,433. The emergency phones, in their current state, are a risk and a liability to the University that must be addressed.

NATURE OF CALLS FROM BLUE PHONES	2014	2015	2016	Total
ALCOHOL VIOL/INTOX SUBJECT	1			1
ANIMAL		1		1
ASSAULT	1	1		2
ASSIST MOTORIST/DISABLED VEHICLE	3	4	3	10
ASSIST OTHER AGENCY	1	1	2	4
DISTURBANCE	1			1
DOMESTIC		2		2
ELEVATOR	14	9	11	34
FIGHT	1			1
FIRE DRILL		1		1
FOUND PROPERTY			1	1
HIT & RUN (PD/PI/F)	1			1
LARCENY	1	1	2	4
MAINTENANCE REQUEST	2		1	3
MEDICAL/FIRST AID	4	2	3	9
MENTAL SUBJECT/SUICIDAL SUBJECT	1		1	2
RAPE			1	1
ROBBERY			1	1
SAFETY ESCORT	21	24	7	52
SECURE/UNSECURE	18	20	16	54
SMOKE REPORTED	1			1

SUSPICIOUS ACTIVITY			1	1
SUSPICIOUS VEHICLE/PERSON	7	11	10	28
TRAFFIC ACCIDENT (PD/PI/F)	1			1
TRAFFIC HAZARD		1		1
VEHICLE STOP			1	1
WATER LEAK / WATER MAIN BREAK	1			1
WELFARE CHECK		1		1
TOTAL	**80**	**79**	**60**	**220**

Repair, Remove, or Replace

We are considering the possibility of reducing the number of the emergency phones and utilizing our mobile safety app as a portable alternative. As suggested by Campus Security Initiative recommendation #19 (see https://www.northcarolina.edu/sites/default/files/unc_campus_security_initiative_report_to_the_president.pdf on page 34), this application provides students with easy access to contact information for reporting and safety related resources, such as campus police and the safety escort service. This will also reduce the current infrastructure cost and offer a more useful and functional solution. However, there may be an issue with the cellular coverage in specific buildings and the availability of mobile phones for everyone.

We recommend continued marketing and implementation of the mobile safety app, considering the conversion of some blue light phones to cellular where coverage allows, and considering the possibility of slowly migrating to touchscreen kiosks that can be used for a variety of reasons including emergencies.

Goal 6: Enhance Security of Campus Communications and Infrastructure

Strategy 6.1 | Evaluate the Effectiveness of the Mass Notification System & Other Methods of communications (e.g., Alertus, WEBS, LiveSafe, Social Media, Flat Panels, & Cisco VoIP)

The UNC Greensboro Police Department has used Blackboard Connect for the past three years to deliver our emergency notifications, timely warnings, and public safety announcements. The system has proven to be reliable, timely, and capable. We are now exploring the possibilities of using other modes of communications (e.g. phone messages, flat panels, and Cisco VoIP) and offering the system to other departments for internal and outreach communications. As our use continues to evolve, we are addressing the multiple Banner data interfaces needed to populate the respective recipients list. Currently, we are working through the various data sets of our individual facilities, campus partners, and outlining institutions (i.e. campus buildings, JSNN, and Union Square). As we continue to refine the use of our notification system, we will adjust our policies and procedures as needed to ensure effectiveness and compliance.

Overall, Blackboard Connect is meeting all of our notification requirements and giving us the versatility to expand the capabilities of our use. The following initiatives should be incorporated in our existing notification system:

- Add flat panels and digital signage
- Integrate the LiveSafe Mobile Security App broadcast feature
- Integrate the Cisco VoIP phones
- Address the inaudible transmission issues with mass notification and WEBS
- Discontinue the use of the Extron intercoms as part of the notification system

Strategy 6.2 | Evaluate the Current Radio Reception in all facilities

Police, fire, and EMS consistently have problems maintaining effective communications while operating in large structures, such as high-rise buildings, apartments, and warehouses. Similar issues exist in structures with a large number of windows (or areas of glass) with reflective coatings. Communications from areas below grade (e.g., basements, parking garages, tunnels) tend to be problematic. It is critical for public safety to communicate with one another within a structure and with units operating outside the structure. Commercial structures are typically built with large amounts of steel and concrete that, to varying degrees, act as barriers to radio frequency waves. In addition, some types of glass and other window materials used in commercial construction inhibit radio frequencies.

For several years, the public safety radios have experienced communications issues in several of the buildings on campus. This includes not only existing buildings but also new construction and major renovations. Currently, the new police department facility is only building on campus with a bi-directional antenna system. There are several others that have historically had problems with transmitting and receiving radio traffic in the building.

Whether communication is via hand-held radio or personal cellular phone, communications to, from, and within structures can degrade depending on a variety of factors. These factors include multipath effects, reflection from coated exterior glass, non-line-of-sight path loss, and signal absorption in the building construction materials, among others. The communications problems may be compounded by lack of a bi-directional antenna to amplify and retransmit the signal. Radio frequency propagation in structures can be so poor that there may be areas where the signal is virtually nonexistent, rendering public safety radio communication impossible.

Strategy 6.3 | Evaluate the Current Cellular Reception on Campus

Although UNCG does not provide cellular phone service, we recognize that cellular coverage is institutionally important for several reasons:

- This is one of several methods the University uses to reach students, faculty, and staff in emergency situations,
- Faculty and staff who have chosen to drop landline service rely on cellular phones for communication for regular business and academic purposes, and
- Students in residence halls rely almost completely on cellular phones for communication.

As reliance on cellular service has grown, some universities across the country have entered into Master Antenna (MA) agreements or built Distributed Antenna Systems (DAS) to improve indoor signal coverage. Both of these methods, or some combination of these methods, promise to provide payments and service enhancements to the universities. However, these methods require a significant capital outlay as well as a requirement for labor hours to coordinate efforts. Given the financial risk and the aesthetic impact to the campus, ITS opted to fund an assessment in a number of UNCG buildings to determine if the University was a good candidate for an MA agreement and/or DAS build.

In the Spring of 2011, the UNCG Center for Geographic Information Science (CGISc) conducted a survey of the indoor mobile phone signal strength in 38 buildings across campus for three major cellular service providers: AT&T, Verizon, and Sprint CDMA. The 38 buildings surveyed by CGISc comprised a total of 2.5 million square feet of space and included 15 residence halls, 10 administrative buildings, and 13 academic buildings. Average building size was 75,000 square feet while the range of interior space was between 13,471 square feet and 196,510 square feet. Although the study identified cellular coverage problems in four buildings on the basement floor, every building floor in the study (with the exceptions noted) had “Acceptable” or better coverage from at least one major cellular service provider. UNCG concluded that we benefit from reasonably good coverage associated with “bleed” from existing infrastructure that the major cellular carriers already have in place, and that opportunities for revenue generation resulting from an MA agreement or DAS implementation are small.

We shared the information on coverage with each of three service providers, showing them only the data for their network. At the time, Sprint did not have plans for additional cellular towers in the area but did commit to assessing the coverage provided by the antenna on the Jackson Library to see if they could improve the user experience on campus. After the survey, Verizon upgraded to 4G wireless in the Greensboro area as part of their infrastructure improvement plan and began pursuing the build out of a macro site on UNCG’s campus on the Eberhart building; as of November 2, 2016, this construction project is scheduled to begin after contract negotiation is complete.

We shared the information on coverage with multiple entities on campus, including the Emergency Preparedness group. Because UNCG’s approach to emergency communications is based on the premise that no single communication method is sufficient, there was no effort at that time to change our approach. For those areas with least reliable cellular coverage, we considered, and sometimes installed, landlines as an alternate means of emergency communication.

In 2015, we began seeing announcements of new Wi-Fi calling services from major handset vendors and cellular carriers, promising a more standardized and accessible solution for indoor coverage. Cellular carriers are motivated to offload traffic from their congested networks. Today, we are seeing more phones shipped with Wi-Fi calling enabled, and phone owners are noticing that Wi-Fi calling is consuming a portion of their data plan. We believe that we will see widespread use of Wi-Fi calling in the next couple of years, as people upgrade their handsets, making an MA agreement or DAS build out obsolete..

In the interim, we will continue to have areas on campus with less than acceptable cellular coverage. During this time, UNCG should consider:

- Continued inventory and assessment of cellular coverage on campus
- Providing alternate communication methods for those areas without reliable cellular reception
- Providing wireless coverage for those areas without UNCG wireless network coverage

Strategy 6.4 | Provide Stable, Well-Performing Core Enterprise Technology Services

Information Technology Services (ITS) provides core enterprise technology that includes:

- The Campus **Network**. Switches, controllers, firewalls, wiring closets, cables, and other moving parts that function together to provide network connectivity and Internet access for over 16,000 wired and over 125,000 wireless computing devices used by student, faculty and staff who transmit more than 16.2 terabytes of data to/from the Internet and 24.7 terabytes of data between users on campus daily.
- Central Campus **Systems** Infrastructure that hosts UNCG's mission-critical applications. Two Tier 2 data centers, 250 physical servers, 675 virtual machines, 700 terabytes of on-premises storage, 68 terabytes of cloud storage, over 35,000 active user accounts, and other moving parts that function together to enable the platform that operates the University ERP, email, storage, Learning Management Systems, hosting of research and department servers, and a computer lab environment that produces over 190,000 user logons each day.
- **Security** hardware and software components required to protect University networks, systems and data from advanced security threats and meet State financial and IT audit requirements. Devices that monitor network traffic, devices that isolate infected computers, and other part function together as a whole to protect UNCG students, faculty and staff from external cyber threats, rejecting approximately 5 million email messages each month and blocking approximately 3 million attacks per day.

Together these three components are the basic “lights and plumbing” required for almost all campus IT services to function, including the support of the goals and strategies outlined in this Master Security Plan. Network, systems, and security technologies become obsolete on 3- to 7-year lifecycles and must be replaced through multi-year project initiatives for the entire campus. UNCG ITS operates according to an enterprise technology lifecycle management strategy that

- does not leverage “bleeding edge” product adoption to avoid early failure problems
- stretches equipment utilization beyond industry-recommended lifecycles to longer UNCG-specific refresh cycles that balance institutionally-tolerable performance and service degradation against costs
- replaces technology before end of vendor support to avoid institutional security and operational risk

Despite this strategy, UNCG is still recovering from back-to-back budget cuts. Although some level of funding is already provided for most services, annual funding shortfalls exist that will prevent ITS from meeting current service commitment obligations.

The University needs stable, well-performing core enterprise technology services to operate and to provide the foundation required to support new initiatives. To meet this goal, budgets for the core enterprise campus network, systems and security technology need to be adequately funded to cover the service level required to meet campus needs today and have appropriate mechanisms for accommodating annual growth and innovation. These budgets should be revised annually to accommodate both expected and unexpected changes. Initiatives that represent “above the core” services should continue to funded from multiple sources as they have been historically, including any new initiatives that are pursued in this Master Security Plan.

IMPLEMENTATION PLAN

The implementation plan is the second major component of the Master Security Plan. It assigns timelines and budgetary recommendations corresponding to the goals and strategies of the Strategic Plan.

Timeline and Budget Table

Table 1 provides an estimated timeline and budget for the implementation of each goal and strategy within the Strategic Plan. These are projected numbers that will be adjusted as programs mature, initial risk assessments are completed, and specific goals and objectives are refined. Table 2 shows a breakout of cost based on the funding type required.

Table 1: Master Security Plan Implementation Costs, by Task and Fiscal Year

	2017	2018	2019	2020
Goal 1: Centrally Manage Security Risk				
Strategy 1.1 | Centralize the Responsibility for the Security Program				
Programmatic Centralization	Reallocate existing resources			
Strategy 1.2 | Strengthen Existing Electronic Security System				
Hire 1 Technical Support Specialist	$0	Existing resources		
Hire 1 Technical Support Analyst	$70,000	$70,000	$70,000	$70,000
Establish TSD Operating Budget	TBD	TBD	TBD	TBD
Strategy 1.3 | Implement Risk Management Process/Program				
Hire 1 Executive IRM Director	$82,550	$82,550	$82,550	$82,550
Hire 1 Emergency Management Program Manager	$86,000	$86,000	$86,000	$86,000
Hire 1 Emergency Management Program Specialist	$0	$64,300	$64,300	$64,300
Hire 1 Clery Compliance Officer	$0	Existing resources		
Establish EM Operating Budget	$35,000	$40,000	$45,000	$50,000
Strategy 1.4 | Evaluate Current Funding for Security and Develop a Scalable Financial Model for the Future				
Perform financial evaluation of	Integrate into existing budget development process.			

security program				
Goal 2: Enhance Security Awareness through Community Engagement and Education				
Strategy 2.1 | Assign Responsibility for the Safety and Security Awareness Program to the Community Relations Unit within the Police Department				
Performed using existing resources	No additional cost.			
Supplemented by the Position Requested in Strategy 2.2	Cost factored into Strategy 2.2 below			
	2017	**2018**	**2019**	**2020**
Strategy 2.2 | Develop Initial & Recurring Safety and Security Training and Awareness Programs				
Hire 1 Crime Prevention Officer	$59,269	$59,269	$59,269	$59,269
Program Budget	$10,000	$10,000	$10,000	$10,000
Strategy 2.3 | Increase Visibility of Security on Campus				
Hire 2 Uniform Security Officers	$80,000	$80,000	$80,000	$80,000
Expand the Student Rangers Program	$25,000	$25,000	$25,000	$25,000
Strategy 2.4 | Engage the Community				
Hire 1 Community Victim Assistant	Grant Position		$59,269	$59,269
Goal 3: Integrate Security into Planning, Design, Construction, and Facilities Operations				
Strategy 3.1 | Develop Minimum Security Criteria				
Performed by the Safety & Security Sub-Committee	Prioritization of existing Technical Services Division Resources			
Strategy 3.2 | Assimilate Security into the Planning Process				
Performed by the Positions Requested in Strategy 1.2	Prioritization of existing Technical Services Division Resources			
Strategy 3.3 | Incorporate Security into the Design Process				
Performed by the Positions Requested in Strategy 2.2	A function of the Crime Prevention Officer and the Support Services Division.			
Strategy 3.4 | Integrate Security into the Construction Process				
Performed by the Positions Requested in Strategy 2.2	A function of the Crime Prevention Officer and the Support Services Division.			
Strategy 3.5 | Incorporate Security into Facilities Operations				
Performed by existing resources with coordination between departments	A functions of Facilities, Design, and Construction			

Strategy 3.6 | Implement Security Program for Special Events and Risk Mitigation				
Performed by the Positions Requested in Strategy 1.3	A function of the Institutional Risk Management Office			
Goal 4: Implement Measures to Protect Buildings and Ensure Fire Protection				
Strategy 4.1 | Implement Building Security Standard Operating Procedures				
Performed by the Assistant EM Position Requested in Strategy 1.3	A function of the Emergency Management Office			
	2017	**2018**	**2019**	**2020**
Strategy 4.2 | Enhance Building Security with Mechanical Locks and Access Control				
Classroom Locks	Funded in 2016	TBD	TBD	TBD
Complete access control system	$350,000	$350,000	$350,000	$350,000
Rekeying after access control	$15,000	$15,000	$15,000	$15,000
Electronic Access Technician	$0	$60,000	$60,000	$60,000
Strategy 4.3 | Expand Campus Wide Video Surveillance System				
Replace all analog cameras	Funded in 2016	Existing resources		
Install additional IP cameras	Funded in 2016	$100,000	$100,000	$100,000
Additional Access Control Tech	$70,000	$70,000	$70,000	$70,000
Strategy 4.4 | Actively Monitor Electronic Security Systems				
UL Central Station Certification	$3,000	$3,000	$3,000	$3,000
Hire 1 Assistant Telecommunicator Supervisor	$70,000	$70,000	$70,000	$70,000
Strategy 4.5 | Standardize the Fire and Security Alarm Systems for All Facilities on Campus				
Consolidated / Dedicated Signal Shop	Implemented	$75,000	$85,000	$85,000
Replace Areas of Rescue with Cellular Emergency Phone Option	TBD	TBD	TBD	TBD
Replace Panic Buttons with Police Speed Dial Button	$15,000	Existing resources		
Strategy 4.6 | Develop and Sustain Automatic External Defibrillator Program				
Purchase 20 AEDs (including pads, AED/CPR first-aid kit, carrying case, mounting box, and wall sign)	$24,000	$24,000	$24,000	$24,000
Annual Maintenance Budget	$1,220	$2,440	$3,660	$4,880

Goal 5: Enhance Security of Campus Perimeter and Outdoor Spaces				
Strategy 5.1 | Define Campus Perimeter				
Performed by existing resources, with the assistance of other department(s).	Reprioritization of existing resources and allocate a line in project specific budget.			
Strategy 5.2 | Develop Campus Gateways				
Performed by existing resources, with the assistance of other department(s).	Reprioritization of existing resources and allocate a line in project specific budget.			
	2017	**2018**	**2019**	**2020**
Strategy 5.3 | Clearly Delineate All Campus Pathways				
Performed by existing resources, with the assistance of other department(s).	Reprioritization of existing resources and allocate a line in project specific budget.			
Strategy 5.4 | Create Uniform Lighting Standard				
Performed by existing resources, with the assistance of other department(s).	Reprioritization of existing resources and allocate a line in project specific budget.			
Strategy 5.5 | Consistently Apply Security Technologies in Exterior Spaces				
Implemented as opportunities arise	Reprioritization of existing resources and allocate a line in project specific budget.			
Goal 6: Enhance Security of Campus Communications and Infrastructure				
Strategy 6.1 | Evaluate the Effectiveness of the Mass Notification System & Other Methods of Communications (e.g., WEBS, LiveSafe, Flat Panels, Cisco VoIP phones)				
Blackboard Connect Annual Subscription	$18,000	$18,000	$18,000	$18,000
Unified Mass Notification System Integration	$15,000	$15,000	$15,000	$15,000
Strategy 6.2 | Evaluate the Current Radio in All Facilities on Campus				
Bi-Directional Antenna Systems	TBD	TBD	TBD	TBD
Strategy 6.3 | Evaluate the Current Cellular Reception on Campus				
Inventory, assessment and remediation of cellular coverage	TBD	TBD	TBD	TBD
Strategy 6.4 | Provide Stable, Well-Performing Core Enterprise Technology Services * As of 20-DEC-2016, these are average annual shortfalls that do NOT include new growth or required annual institutional maintenance.				

Networks*	$ 364,910	$ 364,910	$ 364,910	$ 364,910
Systems*	380,375	380,375	380,375	380,375
Information Security*	69,409	69,409	69,409	69,409
TOTAL COST				