 **PHYSICAL SECURITY PROTOCOLS AND CERTIFICATION MEASUREMENT FOR SCHOOLS**

**Physical security** describes security measures that are designed to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts. Physical security can be as simple as a locked gym door or as elaborate as multiple layers of barriers, armed security guards and guardhouse placement.

The protocols and how they are measured are described below:

**Overview**

Physical security is primarily concerned with restricting physical access by unauthorized people (commonly interpreted as intruders) to controlled facilities, although there are other considerations and situations in which physical security measures are valuable (for example, limiting access within a facility and/or to specific assets, and environmental controls to reduce physical incidents such as fires and floods). Security inevitably incurs costs and, in reality, it can never be perfect or complete - in other words, security can reduce but cannot entirely eliminate risks. Given that controls are imperfect, strong physical security applies the principle of defense in depth using an appropriate combination of overlapping and complementary controls. For instance, physical access controls for protected facilities are generally intended to:

* deter potential intruders (e.g. warning signs and perimeter markings);
* distinguish authorized from unauthorized people (e.g. using keycards/access badges)
* delay, frustrate and ideally prevent intrusion attempts (e.g. strong walls, door locks and safes);
* detect intrusions and monitor/record intruders (e.g. intruder alarms and CCTV systems); and
* trigger appropriate incident responses (e.g. by staff, security guards and/ or police).

What we measure, and then develop if not in place, is a plan that balances your security controls against your risks, taking into account your current threats and vulnerabilities

**Physical access security measures that are appropriate for a high security prison or a military site are inappropriate in a school, although the principles are similar.** Physical security is not a modern phenomenon. The technology is continually evolving along with the threats. Physical security controls that were considered adequate in the past tend to be insecure today due to advances in the knowledge and capabilities of attackers.

**PHYSICAL SECURITY PROTOCOLS**

**Protocol One: Elements and design**

We have identified the following elements (also known Crime Prevention Through Environmental Design or CPTED) to physical security specifically for schools:

1. **Obstacles,** to frustrate trivial attackers and delay serious ones; to include:
   1. explosion protection;
2. **Detection systems**, such as surveillance systems, alarms, security lighting, security guard patrols or closed-circuit television cameras, to make it likely that attacks will be noticed; and
3. **Security response**, to repel, catch or frustrate attackers when an attack is detected.

In a well-designed system, these features **must complement** each other. There are at least four layers of physical security:

* **Environmental design**
* **Mechanical, electronic and procedural access control**
* **Intrusion detection (with appropriate response procedures)**
* **Personnel Identification (authentication)**

**Protocol Two: Deterrence**

The goal of physical security is to convince potential attackers that the likely costs of attack exceeds the value of making the attack, e.g. that consequences of a failed attack may well exceed the gain. The combination of layered security features establishes the presence of territoriality. The initial layer of security for a campus, building, office, or other physical space uses crime prevention through environmental design to deter threats. Some of the most common examples are also the most basic: warning signs or window stickers, fences, vehicle barriers, vehicle height restrictors, restricted access points, security lighting and trenches. However, even passive things like hedgerows may be sufficient in some circumstances.

**Protocol Three: Access control**

The next layer is mechanical and includes gates, doors, and locks. Key control of the locks becomes a problem with large user populations and any user turnover. Keys quickly become unmanageable, often forcing the adoption of electronic access control. Electronic access control easily manages large user populations, controlling for user life-cycles times, dates, and individual access points. For example a user's access rights could allow access from 0700h to 1900h Monday through Friday and expires in 90 days.  Another form of access control (procedural) includes the use of policies, processes and procedures to manage the ingress into the restricted area. An example of this is the deployment of security personnel conducting checks for authorized entry at predetermined points of entry. This form of access control is usually supplemented by the earlier forms of access control (i.e. mechanical and electronic access control), or simple devices such as physical passes.  An additional sub-layer of mechanical/electronic access control protection is reached by integrating a key management system to manage the possession and usage of mechanical keys to locks or property within a building or campus.

**Protocol Four: Detection**

The third layer is intrusion detection systems or alarm systems. Alarm systems trigger a response when unauthorized access is detected. They consist of sensors including motion sensors, contact sensors, and glass break detectors. In some jurisdictions, law enforcement will not respond to alarms from intrusion detection systems unless the activation has been verified by an eyewitness or video. Policies like this one have been created to combat the 94–99 percent rate of false alarm activation in the United States.

**Protocol Five: Identification**

The last layer is video monitoring systems. Security cameras can be a deterrent in many cases, but their real power comes from incident verification and historical analysis. For example, if alarms are being generated and there is a camera in place, the camera could be viewed to verify the alarms. In instances when an attack has already occurred and a camera is in place at the point of attack, the recorded video can be reviewed. Although the term closed-circuit television (CCTV) is common, it is quickly becoming outdated as more video systems lose the closed circuit for signal transmission and are instead transmitting on IP camera networks.  Advances in information technology are transforming video monitoring into video analysis. For instance, once an image is digitized it can become data that sophisticated algorithms can act upon. As the speed and accuracy of automated analysis increases, the video system could move from a monitoring system to an intrusion detection system or access control system. A video camera could potentially data to a processor that outputs to an electronic lock, making a person's visage the key. When actual design and implementation is considered, there are numerous types of security cameras that can be used for many different applications. **A key factor in risk mitigating identification is that your cameras are placed according to your individual and measured risks, threats, and vulnerabilities**.

**Protocol Six: Human response**

Intertwined in these four layers are faculty, staff, students, and parents. Faculty and staff have a role in all layers. The first layer is for all groups, and has them as observers looking for any type of “out of place” or potentially harmful situation. In the second layer, faculty and staff are responsible to administer and control access to the building(s). In the third layer, faculty/staff are assigned respond to reports of concerns, and/or alarms. The response “force” must be able to arrive on site in less time than it is expected that the attacker will require to breach the barriers. And in the fourth layer, the job of monitoring and analyzing incident reports, local crime statistics, and video usually falls to the security professional and/or school administrator. **Faculty and staff obviously have a role also by questioning and reporting suspicious people**. Aiding in identifying people as known versus unknown are identification systems. Often photo ID badges are used and are frequently coupled to the electronic access control system. Visitors are often required to wear a visitor badge, and **that visitor badge should be provided in a layered system to help mitigate risk.**

**Other physical security tools**

New developments in information and communications technology, as well as new demands on security managers, have widened the scope of physical security apparatus. Fire alarm systems are increasingly becoming based on Internet Protocol, thus leading to them being accessible via local and wide area networks within organizations. Emergency notification is now a new standard in schools, as well as physical security information management (PSIM). A PSIM application integrates all physical security systems in a facility, and provides a single and comprehensive means of managing all of these resources. It consequently saves on time and cost in the effectual management of physical security

**PROTOCOL OBJECTIVES/CERTIFICATION REQUIREMENTS**

If the administration and staff follow directions on how to embedding the protocols of physical security then these objectives will be measured and met successfully.

|  |
| --- |
| CERTIFICATION REQUIREMENTS |
| At least 95% of faculty, staff, students, parents, and 3rd Party Contractors are instructed on how/when to report a concern, and the value of maintaining high levels of awareness |
| Elements and Design Protocol has some sort of policy addressing it’s need and implementation, a procedure to support that policy, that procedure and policy is effective and creates low incident rates, everyone responsible for knowing/implementing the policy and procedure knows their role and task, and proactive actions are assigned to this protocol that best mitigate the school’s individual risks, threats, and vulnerabilities. |
| Administrators document risk reduction actions as they take place |
| At least a two person concern reporting and responding system is in place |
| Deterrence Protocol has some sort of policy addressing it’s need and implementation, a procedure to support that policy, that procedure and policy is effective and creates low incident rates, everyone responsible for knowing/implementing the policy and procedure knows their role and task, and proactive actions are assigned to this protocol that best mitigate the school’s individual risks, threats, and vulnerabilities. |
| Detection Protocol has some sort of policy addressing it’s need and implementation, a procedure to support that policy, that procedure and policy is effective and creates low incident rates, everyone responsible for knowing/implementing the policy and procedure knows their role and task, and proactive actions are assigned to this protocol that best mitigate the school’s individual risks, threats, and vulnerabilities. |
| Identification Protocol has some sort of policy addressing it’s need and implementation, a procedure to support that policy, that procedure and policy is effective and creates low incident rates, everyone responsible for knowing/implementing the policy and procedure knows their role and task, and proactive actions are assigned to this protocol that best mitigate the school’s individual risks, threats, and vulnerabilities. |
| Human Response Protocol has some sort of policy addressing it’s need and implementation, a procedure to support that policy, that procedure and policy is effective and creates low incident rates, everyone responsible for knowing/implementing the policy and procedure knows their role and task, and proactive actions are assigned to this protocol that best mitigate the school’s individual risks, threats, and vulnerabilities. |
| 95% of staff are continually trained throughout the year on the value of maintaining high awareness levels |
| 95% of staff are trained on the necessary increase in awareness levels for sexual predators and/or victims of sexual predators |

**BENEFITS TO THE ORGANIZATION**

In addition to drastically reducing the risk of a crisis even on campus the Physical Security Protocol Certification Service also provides the following benefits:

* Reduced risk of lawsuits.
* Increase of staff Professional Development/Training without requiring increased and inconvenient meeting time.
* Quality staff recruited and retained.
* Parental satisfaction and trust rate increased.
* Operational effectiveness increased.
* Withdrawal of students from schools due to safety and security decreased
* Positive press coverage and community exposure.
* “On Site” rates and additional areas of security safety work will receive a 20% reduction in normal rate fees

**ABOUT NEWDAWN SECURITY**

Founded by a former school principal,NewDawn Security specializes in helping organizations identify, prepare for, and mitigate their common and individual risks. NewDawn Security developed and oversees the Excellence in Safe School Operations (ESSO) Protocol and Certification Program, the Excellence in Safe Post Secondary Campus Operations (ESPSCO) Protocol and Certification Program, the Excellence in Safe Church Operations (ESCO) Protocol and Certification, and the Sexual Predator and Abuse Prevention Protocol and Certification. All of these certification services provide an objective method for measuring and maintaining Safe Operation and Risk Prevention Standards. NewDawn Security puts its name, and its reputation right alongside the schools and organizations they serve to enhance and maintain all aspects of safety and security.

**ADDITIONAL RISK BASED SECURITY MANAGEMENT PROTOCOLS NEWDAWN SECURITY CAN EMBED AT YOUR SCHOOL:**

* Entire Security and Safety Operations Audit
* Active Shooter Prevention Protocol
* Sexual Predator and Abuse Prevention Protocol
* Effective School Wide Discipline Incident Reduction Protocol
* Bullying and Harassment Prevention Protocol
* Gang Prevention Protocol
* Drug/Alcohol Incident Reduction Protocol
* Faculty and Staff Security and Safety Professional Development
* Reduced Risk Operation Protocols of Extra Curricular Events
* Crime/Vandalism Prevention Protocol
* High Quality Crisis Response Protocols
* Monitoring and Reduction Strategies for all Risk, Threat, and Vulnerabilities

**CONCLUSION**

We can now provide schools a proactive, research based, and proven effective protocols to prevent them from ever experiencing the devastation of crisis. Schools do not have to do all the work themselves, and they don’t have to accept all the risk and liability. We gladly are able to share this risk and liability due to the valuable type of program we have developed, and the people we have helping your school embed it into your day-to-day activities. Our main goal will be to make sure we do everything possible to make sure you never experience a crisis abuse situation, or if you already have, you never do again. There is no other company in the World that is currently offering anything like this program, or more importantly have the ability to do the same.

Please feel free to contact me with any questions, and/or to schedule an in person presentation. We look forward to providing you the very best.

Sean Spellecy

Chief Executive Officer

NewDawn Security

888.287.6157