

Recommendations

1. Create a new position responsible for security systems and technology including but not be limited to the development of security technology standards, design standards, oversight of security systems, systems integration and physical security surveys and assessments. This individual would report to the Security Technology Working Group.

Done. Mike Kennedy's position

2. Establish campus-wide security standards. Campus-wide security standards are a promising practice that institutions are implementing as they commit considerable resources to security technology. The overall goal of such standards is to ensure that buildings are "security-smart" given reasonably foreseeable threats and available resources. These standards should include building-specific security technology system designations that specify the types of security systems that the University would expect for specific types of buildings.
3. Assign the Department of Campus Security as the formal operational or "business owner" of security technology and security systems.

Done.

4. Create a Security Technology Working Group. The individual holding the new position referenced in recommendation #1 should chair this committee.

Done. Integrated Security Technology Committee

5. Develop campus-wide security technology system equipment standards. Determine common equipment hardware, manufacturers, models, capacities and software that are easily integrated with other systems at the University.

This will happen after the integrated system, however alarm panels, fire panels and panic devices are already being defined.

6. Select a nationally recognized value added reseller (VAR) with the capacity to meet the needs of the University to purchase and install University-approved security systems while leveraging centralization to reduce overall costs.

This, I would believe is a State issue that needs to addressed

7. Develop comprehensive policies related to each specific security technology. These policies should not only cover the purpose, scope and acceptable use of each technology but also the procurement process.

This will happen after the integrated system has been chosen and as we move forward. Construction Design Guides are already being revised or defined.

8. Engage in a campus-wide assessment to identify and inventory all security systems currently being utilized throughout the University. These should at least include security cameras, intrusion alarms, duress alarms, and electronic access control readers.

This has begun, however the Technical Records II position is critical in making this a success.

9. Wherever possible, make an effort to integrate disparate legacy security systems to one common platform that includes all devices and security system countermeasures that terminate at the Campus Security building. Under the current system, individual departments that have previously installed security systems replace or upgrade these systems on an as needed basis. However, we can only assume that that service, maintenance, and upgrades are completed because the University is not aware of all the systems currently in place. Integrating systems will ensure that all systems are integrated and maximize the University's return on investment.

This is in progress with regards to new camera purchases and installations as well as panic devices and alarm panel installs.

10. As the University embarks on the development of University-wide security standards and facility design standards, we suggest an initiative to ensure that all existing building security systems comply with the new standards. Clearly, this is a process that must be phased in over a period of years based on available time and resources.

This will happen after the integrated system has been chosen.

11. Develop a campus-wide acceptable usage policy for security cameras. This policy should at least include the purpose and scope of the cameras, who has authority over them and their responsibilities, as well as the principles and procedures associated with the cameras.

Done. BSU Policy #12140

12. Develop security camera equipment design standards that detail the minimum requirements, i.e. whether the cameras should be analog, IP, day/night/ color, megapixel, fixed, PTZ, etc., as well as mandatory camera locations, and minimum recording rates.

This will happen after the integrated system has been chosen.

13. Develop video management system requirements that include retention periods, data security protocols, video retrieval, distribution and chain of custody.

Done. BSU Policy #12140

14. Install additional security cameras based on the phased roll-out described earlier in this section of the assessment.

This will be taken into consideration

15. Develop an alarm installation and monitoring policy.

This is in progress. BSU Policy #12150 for panic devices is in place.

16. Consider requiring all intrusion alarms to report directly to Campus Security.

This is in progress. However off campus locations such as TECenter in Nampa, Bronoc Shops in Nampa, Meridian and Twin Falls need further discussion.

17. Consider reallocating alarm fees currently paid to third party vendors to Campus Security to maintain and support alarm-monitoring activities.

In progress. With the new GSM Dialers and Manitou software, 3rd party vendor will no longer be used.

18. Develop facility and equipment standards for the use of intrusion detection systems.

In progress.

19. Develop a risk-based decision matrix to determine where alarms should be installed and what type of alarms should be approved for installation.

Future project

20. Continue to expand the use of door prop, forced and held open alarms in all residential and high-risk facilities.

On-going. A new access control system will be the next major project and the system choice is dependent upon the integrated camera system.