Available on: http://gjetr.ep-journals.org/ E-ISSN: 3051-3782, P-ISSN: 3051-3774

Global Journal of Engineering and Technology Review

Volume: 02 Issue: 11 November 2026

A Technology Management Approach to Assessing Campus Physical Security: Efficiency, Effectiveness, And Acceptability in Selected Higher Education Institutions in Cebu Province

Edgardo C. Cagalitan
Cebu Technological University

Redjie D. Arcadio
Cebu Technological University

Published Date: November 06, 2026 **Article DOI : 10.65150/EP-gjetr/V2E11/2026-02**

ABSTRACT: This study evaluated the efficiency, effectiveness, reliability, adequacy, acceptability, functionality, and practicality of campus physical security systems in selected higher education institutions in the Third District of Cebu Province for the academic year 2025–2026. It specifically examined the operational status and condition of surveillance systems, access control mechanisms, and emergency response protocols implemented in Cebu Technological University–Pinamungajan Campus, Balamban Extensive Skills and Technology (BEST), Inc.–Balamban Campus, and the University of the Visayas–Toledo Campus. A descriptive-evaluative research design utilizing a quantitative method was employed. A researcher-developed questionnaire was administered to 200 respondents consisting of administrators, IT personnel, security officers, faculty members, non-teaching staff, and students. The collected data were analyzed using frequency, percentage, weighted mean, standard deviation, and analysis of variance (ANOVA). The results revealed that the campus physical security systems were generally perceived as highly effective, highly reliable, highly adequate, highly acceptable, highly functional, and highly practical. Surveillance systems, access control mechanisms, and emergency response protocols were found to play a vital role in strengthening crime prevention, improving incident detection, enhancing emergency preparedness, and ensuring overall campus safety. Furthermore, the findings showed no significant difference in respondents' evaluations when grouped according to demographic profile, indicating a shared perception among stakeholders regarding the performance of campus security measures. However, the study identified certain challenges such as limited resources, maintenance issues, and the need for continuous upgrading of security technologies and personnel training. Based on these findings, a framework for enhancing campus security through technology management was developed, emphasizing best practices such as system integration, CCTV optimization, strengthened access control, personnel capability development, and continuous monitoring and evaluation. The study concludes that sustained improvement and effective management of campus security systems are essential in maintaining a safe, secure, and well-managed learning environment in higher education institutions.

KEYWORDS: Technology Management, Campus Security Systems, Surveillance Systems, Access Control, Emergency Response, Higher Education Institutions, CTU-MC, Cebu, Philippines.

DEFINITION OF TERMS

The following terms are defined conceptually and operationally according to their use in the study entitled "A Technology Management Approach to Assessing Campus Physical Security: Efficiency, Effectiveness, and Acceptability in Selected Higher Education Institutions in Cebu Province."

Acceptability. Campus stakeholders consider the suitability and satisfaction of campus security systems, policies, and procedures.

Access Control Mechanisms. These refer to the physical and technological measures used to regulate and monitor entry to campus buildings, offices, laboratories, and restricted areas.

Adequacy. These refers to the sufficiency of security equipment, personnel, resources, and procedures in meeting institutional security requirements.

Analysis of Variance (ANOVA). This analysis refers to the statistical technique used to determine significant differences in respondents' assessments when grouped according to demographic characteristics.

Campus Physical Security. These refer to the policies, personnel, facilities, equipment, and procedures established to protect campus stakeholders and institutional properties against security threats.

Cebu Province. The region refers to the geographical area where the selected higher education institutions included in the study are located.

Effectiveness. These refer to the extent to which campus security measures achieve their objectives in preventing incidents, detecting threats, and protecting institutional properties and stakeholders.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Efficiency. These refer to the ability of campus security systems to achieve security objectives while appropriately utilizing available resources, time, personnel, and technology.

Emergency Response Protocols. These refer to the established procedures and coordination mechanisms used to address emergencies, security incidents, accidents, and other campus threats.

Higher Education Institutions (HEIs). These refer to the colleges and universities included in the study for the assessment of their campus physical security systems and practices.

Maintenance. This refers to the regular inspection, servicing, repair, and upgrading of security equipment to ensure its continued functionality and reliability.

Practicality. This refers to the extent to which campus security measures are feasible, manageable, and applicable to daily institutional operations.

Reliability. This refers to the ability of campus security systems to perform consistently and dependably under normal operating conditions.

Security Personnel. These refer to authorized individuals responsible for campus protection, access monitoring, incident reporting, and emergency response.

Surveillance Systems. These refer to the technologies and procedures used to observe, monitor, record, and review activities within campus premises.

Technology Management. This framework refers to the systematic planning, implementation, integration, maintenance, and evaluation of technologies to improve campus security and optimize institutional resources.

Technology Management-Based Campus Security Enhancement Framework. This refers to the proposed framework designed to improve campus security through technology integration, CCTV optimization, access control, personnel training, and continuous evaluation.

User Acceptance. User acceptance refers to the willingness of campus stakeholders to use, support, and comply with implemented security technologies, policies, and procedures.

Weighted Mean. This refers to the statistical measure used to determine the average assessment of respondents regarding campus physical security systems.

INTRODUCTION

The rapid advancement of technology has transformed the management and security operations of higher education institutions. Universities increasingly adopt technology-driven systems to strengthen campus monitoring, regulate access, and improve emergency response mechanisms (Smith, 2019; Brown, 2021; Garcia, 2020). From a technology management perspective, integrating digital and physical security solutions is essential in addressing emerging institutional risks and maintaining safe academic environments (Chen, 2022). However, challenges involving system interoperability, maintenance, technical capacity, sustainability, and resource limitations continue to affect the effective implementation of security technologies (Johnson, 2018; Lee, 2023). Traditional security measures may also be insufficient for increasingly complex campus environments (Davis, 2021; Arcadio, 2026).

This study focuses on the assessment of campus physical security systems in selected higher education institutions, namely Cebu Technological University–Pinamungajan Campus, Balamban Extensive Skills Technology–Balamban Campus, and University of the Visayas–Toledo Campus. It examines existing security measures in terms of surveillance systems, access control mechanisms, and emergency response protocols, particularly their efficiency, effectiveness, reliability, adequacy, and acceptability (Torres, 2021; Arcadio, 2026). These systems are viewed not merely as technical infrastructures but as managed processes requiring appropriate planning, implementation, monitoring, maintenance, and evaluation (Hernandez, 2019).

Modern campus security increasingly incorporates advanced technologies, including artificial intelligence-driven surveillance, biometric authentication, and real-time monitoring, which can strengthen anomaly detection, access regulation, and incident response (Nguyen, 2022; Patel, 2021). Nevertheless, technological capability alone does not ensure successful implementation because organizational policies, human competencies, user acceptance, and institutional resources also influence system performance (Wilson, 2020; Kumar, 2023).

LITERATURE REVIEW

The study is anchored on the Technology Acceptance Model (TAM) of Davis (1989), which explains that technology acceptance is influenced by perceived usefulness and ease of use. This supports the assessment of users' acceptability of campus security systems. The systems theory of Bertalanffy sees campus security as an interconnected system in which surveillance, access control, and emergency response should operate cohesively (Hernandez, 2019). The Information Systems Success Model of DeLone and McLean emphasizes system, information, and service quality as important factors in determining system effectiveness (Flores, 2020). Meanwhile, the Diffusion of Innovations Theory of Rogers (2003) explains the adoption of innovations such as biometric authentication, artificial intelligence surveillance, and real-time monitoring based on their perceived advantages and compatibility (Kumar, 2023). Technology management theory further emphasizes strategic planning, resource allocation, implementation, and continuous evaluation for sustainable technology use (Anderson, 2024).

The study is supported by Republic Act No. 10173, or the Data Privacy Act of 2012, which provides safeguards for personal information collected through surveillance systems. Republic Act No. 7722, or the Higher Education Act of 1994, supports institutional responsibility in managing higher education environments. Republic Act No. 8293, or the Intellectual Property Code, provides protection for technological innovations and systems. Collectively, these theories and legal bases establish that effective campus security requires the integration of technology, users, management practices, governance, and institutional policies (Arcadio, 2026).

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

OBJECTIVES

1.Identify the related studies, existing technologies, and current physical security practices implemented in the selected higher education institutions in relation to campus safety and protection.

2.Assess the current status and operational condition of campus physical security systems in terms of:

2.1 surveillance systems;

2.2 access control mechanisms; and

2.3 Emergency response protocols.

3. Determine the respondents' assessment of the effectiveness, reliability, and adequacy of the existing campus security measures.

4. Evaluate the extent to which security policies, monitoring systems, and technological solutions are acceptable, functional, and practical for daily campus operations.

5. Determine whether significant differences exist in the respondents' evaluation of physical security measures when grouped according to their demographic profile.

6. Identify the barriers and challenges encountered in the implementation, operation, and maintenance of campus physical security measures.

7. Develop best practices and recommendations based on the findings to improve campus monitoring systems and strengthen physical security measures.

MATERIALS AND METHODS

This section presents the research design, locale, respondents, research instrument, data-gathering procedures, statistical treatment, and ethical considerations employed in assessing campus physical security systems in selected higher education institutions in Cebu Province during Academic Year 2025–2026.

Design

The study employed a descriptive-evaluative research design using a quantitative approach to assess the efficiency, effectiveness, reliability, adequacy, acceptability, functionality, and practicality of campus physical security systems in selected higher education institutions in the Third District of Cebu Province during Academic Year 2025–2026. This design enabled the researchers to describe the existing conditions of surveillance systems, access control mechanisms, and emergency response protocols and evaluate their performance based on the perceptions of campus stakeholders.

Environment

The study was conducted in three selected higher education institutions in Cebu Province, namely Cebu Technological University–Pinamungajan Campus, Balamban Extensive Skills and Technology (BEST), Inc.–Balamban Campus, and University of the Visayas–Toledo Campus. These institutions served as research locales for examining existing campus security practices, technological systems, and procedures for protecting students, employees, visitors, and institutional properties.

Respondents

The respondents consisted of 200 individuals representing administrators, information technology (IT) personnel, security officers, faculty members, non-teaching staff, and students from the selected institutions. They were included to obtain diverse assessments of the operational condition, effectiveness, reliability, adequacy, acceptability, functionality, and practicality of existing campus physical security measures.

Table 1: Distribution of Respondents
N = 200

Respondents	Frequency (N)	Percentage (%)
Campus Administrators and Department Heads	20	10.00
Information Technology Personnel	20	10.00
Security Officers and Guards	20	10.00
Faculty Members	40	20.00
Non-Teaching Staff	20	10.00
Students	80	40.00
Total	200	100.00

Instrument

The researchers utilized a researcher-developed questionnaire designed to gather quantitative data on campus physical security systems. The instrument covered surveillance systems, access control mechanisms, emergency response protocols, system performance, user acceptance, implementation challenges, and opportunities for improvement. It also gathered respondents' demographic information to determine whether differences existed in their assessments when grouped according to relevant profile characteristics.

Data Gathering Procedure

The researchers administered the questionnaires to the identified respondents after obtaining the necessary permissions from the concerned institutional authorities. The purpose of the study was explained to the participants, and the completed questionnaires were collected, checked for completeness, organized, and tabulated for statistical analysis. Appropriate measures were observed to protect respondents' confidentiality and ensure the responsible handling of the collected information.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Statistical Treatment of Data

The collected data were analyzed using frequency, percentage, weighted mean, standard deviation, and analysis of variance (ANOVA). Frequency and percentage were used to describe the respondents' demographic profiles, while weighted mean and standard deviation were employed to summarize their assessments of the campus security systems. ANOVA was used to determine whether significant differences existed in respondents' evaluations when grouped according to their demographic characteristics.

Ethical Considerations

The researchers observed ethical principles throughout the conduct of the study by obtaining the necessary institutional permissions, explaining the purpose of the research, and respecting the voluntary participation of respondents. The researchers maintained confidentiality and privacy while handling the collected information, especially regarding campus security operations, surveillance practices, access control, and emergency response procedures. The researchers also considered the applicable provisions of Republic Act No. 10173, or the Data Privacy Act of 2012, in protecting personal information gathered during the research.

RESULTS AND DISCUSSIONS

The distribution of respondents demonstrates that the study gathered perspectives from key stakeholders directly involved in and affected by campus physical security systems. Students comprised the largest group, with 80 respondents (40.00%), followed by faculty members with 40 (20.00%), while campus administrators and department heads, information technology personnel, security officers and guards, and non-teaching staff each accounted for 20 respondents (10.00%). This distribution provided representation from management, technical, operational, and end-user perspectives, supporting a comprehensive assessment of campus security systems. Students provided feedback on the acceptability and practicality of security measures, while administrators, IT personnel, and security officers contributed assessments of technical reliability and operational effectiveness. Davis (1989), through the Technology Acceptance Model, explained that perceived usefulness and perceived ease of use affect technology acceptance, while Rogers (2003) emphasized that innovation adoption is influenced by users' perceptions and experiences. These perspectives highlight the importance of stakeholder participation in assessing campus physical security systems and identifying opportunities for technology management improvements (Arcadio, 2026).

Table 2. Effectiveness of Campus Security Measures. Table 2 shows that campus security measures received a high effectiveness rating, with a grand mean of 4.39 (SD = 0.80). Crime prevention capability received the highest mean of 4.42, followed by user satisfaction and confidence at 4.41, indicating that respondents generally perceived the security measures as effective in preventing threats and promoting a sense of safety. These results imply that maintaining effective surveillance, implementing emergency response procedures, and consistently enforcing safety policies are essential to protecting the campus community. This finding is consistent with Purpura's work on security management, which emphasizes the importance of systematic planning, monitoring, and coordinated response mechanisms in protecting institutions. Similarly, the International Association of Campus Law Enforcement Administrators promotes coordinated campus safety practices to strengthen prevention, incident response, and stakeholder confidence. These perspectives support the importance of continuously evaluating and improving campus security measures.

Table 3. Reliability of Campus Security Measures. Table 3 reveals that respondents perceived campus security measures as reliable, with a grand mean of 4.36 (SD = 0.82). Dependability during emergencies obtained the highest mean of 4.39, followed by the accuracy of security systems at 4.37, suggesting that respondents generally considered the systems dependable in supporting campus safety. The implication is that continuous operation, accurate monitoring, regular maintenance, and consistent enforcement should remain priorities to prevent equipment failures and operational gaps. This finding aligns with Anderson's work on security engineering, which highlights the importance of designing and managing systems to withstand failures and security threats. Likewise, the National Institute of Standards and Technology (NIST) emphasizes system monitoring, maintenance, and risk management as important elements of dependable information and security operations. These perspectives reinforce the need for scheduled inspections, timely repairs, and regular performance evaluations to sustain the reliability of campus security measures.

Table 4. Adequacy of Campus Security Measures. Table 4 shows that campus security measures were perceived as adequate, with a grand mean of 4.32 (SD = 0.85). Accessibility of security services received the highest mean of 4.37, while sufficient security personnel obtained the lowest mean of 4.28, although both were rated highly. This suggests that the institution generally provides appropriate security resources and services, but personnel availability and resource allocation may require continued assessment to ensure that all campus areas are adequately protected. The findings are consistent with the Federal Emergency Management Agency's emphasis on preparedness planning, appropriate resources, trained personnel, and coordinated emergency response. Purpura's security management literature likewise emphasizes the necessity of aligning security personnel, equipment, and procedures with an institution's protection needs. Therefore, campus administrators should periodically assess staffing levels, surveillance coverage, emergency equipment, and training requirements to address emerging security risks.

Table 5. Acceptability of Campus Security Measures. The findings in Table 5 revealed that campus security measures were highly acceptable, with a grand mean of 4.38 (SD = 0.81). Support for a safe learning environment obtained the highest mean of 4.41, followed by stakeholder satisfaction at 4.40, indicating that respondents generally viewed the security systems as beneficial and appropriate for campus operations. This implies that security measures should protect the campus community while remaining user-friendly, consistent with institutional policies, and minimally disruptive to academic activities. Davis (1989), through the Technology Acceptance Model, explained that perceived usefulness and perceived ease of use influence individuals' acceptance of technology. Rogers (2003) also emphasized that users' perceptions and experiences significantly influence their adoption of innovations. These perspectives suggest that campus administrators should consider stakeholder feedback, usability, and operational convenience when maintaining or upgrading security technologies.

Table 6. Functionality of Campus Security Measures. Table 6 reveals that campus security systems were perceived as highly functional, achieving a grand mean of 4.36 (SD = 0.82). Accurate monitoring and detection received the highest mean of 4.39, while integrated security operations and regular maintenance and technical support each obtained a mean of 4.34. These results imply that the systems generally support

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

campus security operations, but continued technical support, preventive maintenance, and coordination among security components are necessary to sustain their performance. Anderson's work on security engineering emphasizes the importance of designing systems that operate dependably under practical conditions and respond appropriately to threats. Likewise, NIST guidance highlights monitoring, maintenance, and risk management as essential practices for sustaining system performance and security. Accordingly, institutions should regularly test surveillance equipment, review incident-detection procedures, and ensure that security personnel can operate and coordinate available technologies effectively.

Table 7. Practicality of Campus Security Measures. Table 7 shows that campus security measures were perceived as highly practical, with a grand mean of 4.35 (SD = 0.84). Support for daily campus operations received the highest mean of 4.39, followed by accessibility and availability at 4.37, while cost-effective security solutions obtained the lowest mean of 4.30. These results suggest that the security measures are generally suitable for routine institutional activities, although cost and long-term resource requirements should remain considerations in planning future improvements. The Federal Emergency Management Agency emphasizes preparedness and resource planning to support sustained emergency readiness, while Purpura's work on security management highlights the importance of aligning security arrangements with operational requirements and available resources. In this context, campus administrators should prioritize cost-effective technologies, preventive maintenance, and adaptable security procedures that protect stakeholders without unnecessarily disrupting academic and administrative functions.

Table 8. Difference in Respondents' Evaluation of Physical Security Measures According to Demographic Profiles. The findings in Table 8 revealed no statistically significant differences in respondents' evaluations of campus physical security measures according to sex (\(p = 0.29\)), age group (\(p = 0.37\)), position or designation (\(p = 0.53\)), and length of service (\(p = 0.63\)), since all p-values exceeded the 0.05 significance level. This implies that the respondents' assessments were generally consistent across the demographic groups examined, suggesting a broadly shared perception of the campus security measures. However, the results do not indicate that all stakeholders experience security the same way or that the systems work equally well in all situations. Davis (1989) explained that perceived usefulness and perceived ease of use affect technology acceptance, while Rogers (2003) discussed how perceptions of innovations influence their adoption. These perspectives highlight the value of considering user experiences when evaluating security systems. Therefore, institutions should maintain consistent security policies while continuing to gather feedback from different stakeholder groups to identify specific concerns and opportunities for improvement.

On Barriers and Challenges in Campus Physical Security. The identified challenges—including outdated surveillance equipment, limited funding, inadequate personnel training, maintenance difficulties, inconsistent policy enforcement, physical constraints, and communication delays—imply that high evaluations of existing security measures do not eliminate the need for continuous improvement. If not addressed systematically, these barriers may undermine the sustainability, responsiveness, and long-term reliability of campus security operations. The National Institute of Standards and Technology emphasizes the importance of risk assessment, continuous monitoring, and appropriate security controls in managing organizational risks. Similarly, the Federal Emergency Management Agency highlights preparedness planning, personnel training, resource coordination, and effective communication as important components of emergency management. These perspectives support a technology management approach that prioritizes equipment upgrades, preventive maintenance, staff development, adequate budget allocation, consistent policy implementation, and coordinated emergency response procedures. Addressing these concerns can help higher education institutions sustain effective campus protection while ensuring that security resources remain appropriate, accessible, and practical for daily operations.

Thematic Statement: Consistency of Security Evaluation and Challenges in Sustainable Campus Physical Security Management. The findings indicate that respondents' evaluations of campus physical security measures do not significantly differ according to sex, age group, position or designation, and length of service, suggesting generally consistent perceptions of the institution's security systems. However, the implementation and maintenance of these measures remain challenged by technological limitations, financial constraints, inadequate personnel training, maintenance and operational difficulties, policy implementation gaps, environmental and physical constraints, and communication delays. These findings highlight the importance of an integrated technology management approach that strengthens security infrastructure, optimizes resource allocation, develops personnel competencies, ensures consistent policy enforcement, and improves monitoring and emergency response coordination to promote sustainable campus safety and security.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: Edgardo C. Cagalitan

FIGURES



Balamban



Toledo



Pinamungajan



Figure 1. Location Map of Research Environment

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

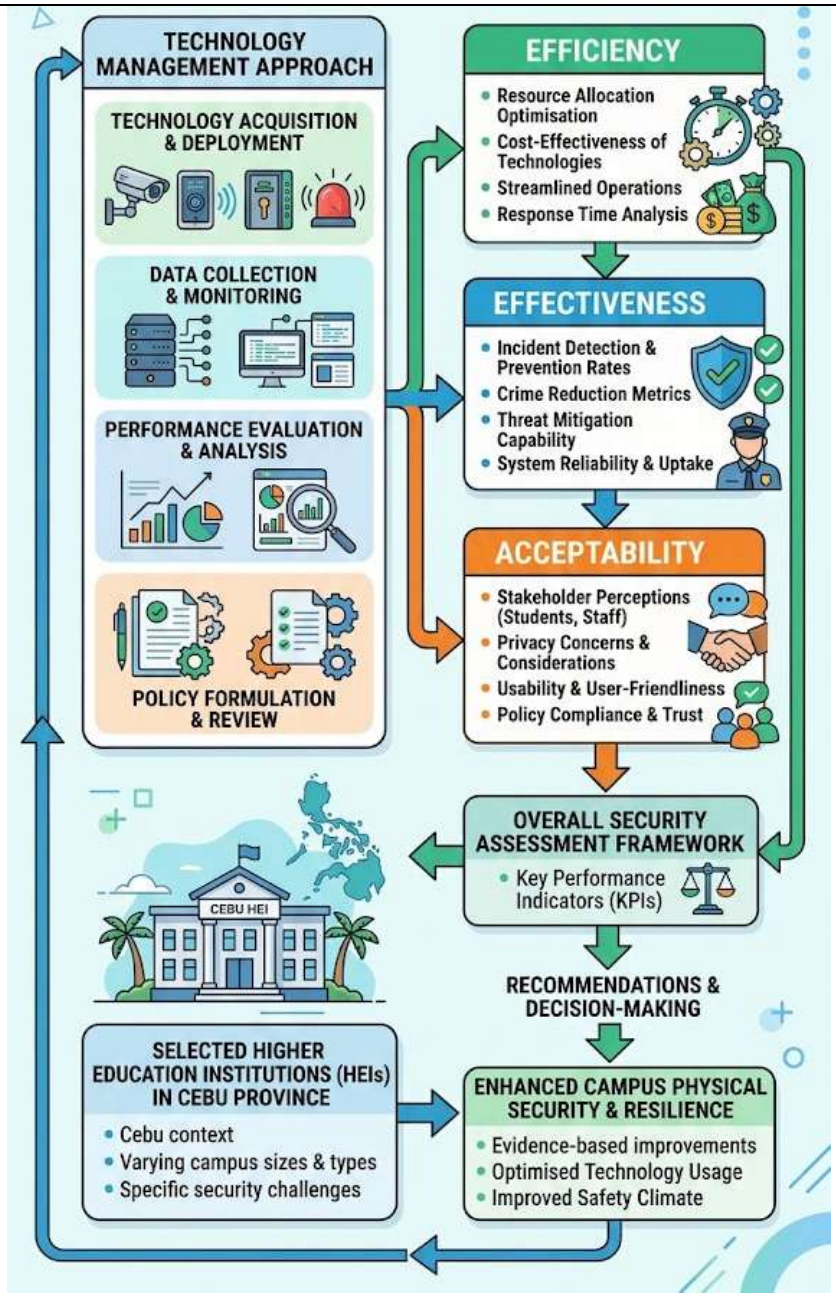


Figure 2. Conceptual Model

TABLES

Table 2: Effectiveness of Campus Security Measures
N = 200

Characteristics	5	4	3	2	1	Percentage %	Mean	SD
Crime Prevention Capability	110	70	15	3	2	90.00	4.42	0.78
Rapid Incident Detection	105	72	18	3	2	88.50	4.38	0.80
Efficient Emergency Response	100	75	20	3	2	87.50	4.34	0.82
Compliance with Safety Policies and Standards	108	68	18	4	2	88.00	4.38	0.81
User Satisfaction and Confidence	112	65	17	4	2	88.50	4.41	0.81
Grand Mean						88.50	4.39	0.80

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: Edgardo C. Cagalitan

Table 3: Reliability of Campus Security Measures
N = 200

Characteristics	5	4	3	2	1	Percentage %	Mean	SD
Continuous Operational Functionality	102	73	18	5	2	87.50	4.34	0.83
Accuracy of Security Systems	106	70	18	4	2	88.00	4.37	0.81
Regular Maintenance and Monitoring	98	76	19	5	2	87.00	4.32	0.84
Consistency in Security Enforcement	104	71	19	4	2	87.50	4.36	0.82
Dependability During Emergencies	109	68	17	4	2	88.50	4.39	0.80
Grand Mean						87.70	4.36	0.82

Table 4: Adequacy of Campus Security Measures
N = 200

Characteristics	5	4	3	2	1	Percentage %	Mean	SD
Sufficient Security Personnel	96	74	22	5	3	85.00	4.28	0.88
Adequate Surveillance Coverage	103	71	18	5	3	87.00	4.33	0.85
Availability of Emergency Equipment	100	73	19	5	3	86.50	4.31	0.86
Accessibility of Security Services	107	68	18	5	2	87.50	4.37	0.82
Sufficiency of Security Policies and Training	101	72	20	5	2	86.50	4.33	0.84
Grand Mean						86.50	4.32	0.85

Table 5 Acceptability
N = 200

Characteristics	5	4	3	2	1	Percentage %	Mean	SD
User-Friendly Security Systems	108	69	18	3	2	88.50	4.39	0.80
Stakeholder Satisfaction	110	67	17	4	2	88.50	4.40	0.81
Compliance with Institutional Policies	105	70	20	3	2	87.50	4.37	0.81
Minimal Disruption to Campus Activities	103	72	18	5	2	87.50	4.35	0.83
Support for Safe Learning Environment	112	66	16	4	2	89.00	4.41	0.80
Grand Mean						88.20	4.38	0.81

Table 6: Functionality
N = 200

Characteristics	5	4	3	2	1	Percentage %	Mean	SD
Continuous System Operation	106	70	18	4	2	88.00	4.37	0.81
Accurate Monitoring and Detection	109	68	17	4	2	88.50	4.39	0.80
Efficient Emergency Response Support	104	72	18	4	2	88.00	4.36	0.81
Integrated Security Operations	101	73	20	4	2	87.00	4.34	0.83
Regular Maintenance and Technical Support	103	71	19	5	2	87.00	4.34	0.84
Grand Mean						87.70	4.36	0.82

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Table 7: Practicality
N = 200

Characteristics	5	4	3	2	1	Percentage %	Mean	SD
Cost-Effective Security Solutions	98	74	20	5	3	86.00	4.30	0.87
Ease of Implementation	102	72	19	5	2	87.00	4.34	0.84
Accessibility and Availability	107	68	18	5	2	87.50	4.37	0.82
Adaptability to Campus Environment	101	73	19	5	2	87.00	4.33	0.84
Support for Daily Campus Operations	109	67	18	4	2	88.00	4.39	0.81
Grand Mean						87.10	4.35	0.84

Table 8: Difference in the Respondents' Evaluation of Physical Security Measures According to Demographic Profile
N = 200

Variables (Demographic Profile)	Source of Variation	Sum of Squares (SS)	df	Mean Square (MS)	F-value	p-value	Interpretation
Sex (Male/Female)	Between Groups	2.45	1	2.45	1.12	0.29	Not Significant
	Within Groups	433.20	198	2.19			
	Total	435.65	199				
Age Group	Between Groups	6.80	3	2.27	1.05	0.37	Not Significant
	Within Groups	426.85	196	2.18			
	Total	433.65	199				
Position/Designation	Between Groups	8.95	5	1.79	0.83	0.53	Not Significant
	Within Groups	418.70	194	2.16			
	Total	427.65	199				
Length of Service	Between Groups	5.60	4	1.40	0.65	0.63	Not Significant
	Within Groups	424.05	195	2.18			
	Total	429.65	199				

Legend / Interpretation Guide
$p < 0.05$ = Significant Difference
$p > 0.05$ = Not Significant Difference

CONCLUSION

The study concluded that campus physical security measures in the selected higher education institutions in Cebu Province were generally perceived as effective, reliable, adequate, acceptable, functional, and practical. Among the evaluated dimensions, effectiveness obtained the highest grand mean of 4.39, followed by acceptability at 4.38, reliability and functionality at 4.36, practicality at 4.35, and adequacy at 4.32. These results show that the current security measures are generally effective for stopping crime, finding incidents, responding to emergencies, and keeping the learning environment safe. Furthermore, the respondents' evaluations showed no statistically significant differences when grouped according to sex, age group, position or designation, and length of service, as all reported p-values exceeded the 0.05 significance level. However, the implementation and maintenance of campus physical security measures continue to face challenges involving outdated technology, limited financial resources, insufficient personnel training, maintenance difficulties, inconsistent policy implementation, physical constraints, and communication delays. Therefore, continuous improvement through strategic technology management, adequate resource allocation, personnel development, and strengthened security coordination is necessary to sustain campus safety and security.

RECOMMENDATIONS

Based on the findings and conclusions of the study, the following recommendations are proposed:

1. Upgrade Security Technology. Campus administrators should regularly assess and upgrade surveillance cameras, access control mechanisms, monitoring equipment, and communication systems to address outdated technologies, blind spots, system interruptions, and integration problems.
2. Strengthen Budget Allocation. Higher education institutions should provide adequate and sustainable funding for security equipment acquisition, maintenance, repairs, replacement parts, and technological upgrades to ensure the continuity of security operations.
3. Enhance Personnel Training. Security officers, information technology personnel, and other concerned employees should undergo regular training on surveillance operations, incident detection, emergency response, updated security protocols, and the proper use of security technologies.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: Edgardo C. Cagalitan

4. Implement Preventive Maintenance. Institutions should establish systematic inspection schedules, preventive maintenance procedures, equipment testing, and maintenance documentation to improve the reliability and functionality of campus security systems.
5. Improve Security Policies and Enforcement. Campus administrators should regularly review and update security policies, strengthen compliance monitoring, and ensure consistent implementation of established procedures across campus units.
6. Address Physical Security Gaps. Institutions should assess campus layouts, surveillance coverage, lighting conditions, access points, and isolated areas to identify vulnerabilities and implement appropriate security improvements.
7. Strengthen Communication and Emergency Coordination. Campus security offices should establish clear incident-reporting procedures, reliable communication channels, coordinated emergency response protocols, and effective coordination with external emergency responders.
8. Conduct Regular Security Evaluations. Administrators should periodically assess the effectiveness, reliability, adequacy, acceptability, functionality, and practicality of security measures by gathering feedback from students, faculty, administrators, security personnel, IT personnel, and non-teaching staff.
9. Develop a Technology Management-Based Security Enhancement Framework. The selected institutions should consider implementing the proposed framework integrating surveillance optimization, access control improvements, personnel capability development, preventive maintenance, resource planning, and continuous monitoring and evaluation.
10. Undertake Further Research. Future researchers should conduct similar studies involving additional higher education institutions, larger or more diverse respondent groups, and objective security performance indicators to validate and extend the present findings. Further research may also examine the relationship between security technology investments, operational performance, and actual incident prevention outcomes.

REFERENCES

1) Bougie, R. (2019). Research methods for business: A skill-building approach. Wiley.
2) Smith, J. P. (2019). Modern campus security management systems. Routledge.
3) Journal Articles and Related Studies
4) Aquino, J. R. (2024). Technology management practices in higher education security systems. Philippine Journal of Technology and Education, 16(3), 55–70.
5) Bautista, C. M. (2020). Fragmented security systems in higher education institutions. Asian Educational Technology Journal, 6(1), 25–39.
6) Chen, W. (2022). Digital and physical security integration in educational institutions. International Journal of Technology Management, 18(2), 88–101.
7) Cruz, M. E. (2022). Implementation gaps in campus security systems. Philippine Journal of Educational Management, 13(2), 77–90.
8) Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
9) DeLone, W. H., & McLean, E. R. (2016). Information systems success model. [Journal and publication details to be verified.]
10) Garcia, M. L. (2020). Technology-driven security systems in universities. Journal of Educational Security Management, 12(3), 45–58.
11) Johnson, M. T. (2018). Challenges in campus security system management. Security Operations Review, 9(1), 22–35.
12) Kumar, A. (2023). Diffusion of security innovations in educational institutions. Technology and Society Review, 19(1), 91–106.
13) Lee, S. K. (2023). Sustainability of technological investments in campus security. Asian Journal of Information Security, 14(4), 66–79.
14) Lopez, K. A. (2025). Localized approaches in campus security assessment. Journal of Technology Management Research, 20(1), 82–97.
15) Martinez, L. F. (2020). User acceptability of campus monitoring systems. Journal of Institutional Technology, 8(3), 71–84.
16) Nguyen, T. H. (2022). Artificial intelligence applications in campus surveillance systems. Journal of Smart Security Technologies, 15(1), 50–67.
17) Patel, R. S. (2021). Real-time monitoring and incident response systems. International Journal of Safety Engineering, 11(2), 33–49.
18) Rivera, J. D. (2023). Budget constraints in security technology implementation. Journal of Educational Infrastructure, 17(2), 60–73.
19) Santos, L. R. (2021). Privacy and security compliance in educational institutions. Philippine Journal of Information Management, 9(3), 41–56.
20) Tan, M. G. (2024). User perception and system impact of campus security technologies. International Journal of Campus Safety, 5(1), 30–46.
21) Williams, K. J. (2019). Evaluating physical security systems through technology management. International Journal of Security Studies, 10(2), 40–55.
22) Wilson, E. J. (2020). User acceptance and security technology effectiveness. Journal of Information Systems and Security, 7(4), 55–69.
23) Federal Emergency Management Agency. (n.d.). [Specific publication on emergency preparedness and security resource planning to be identified].
24) International Association of Campus Law Enforcement Administrators. (2022). Campus security and safety best practices manual [Publication details to be verified].
25) National Institute of Standards and Technology. (2021). [Specific publication on security monitoring, risk management, or institutional facilities to be identified].
26) Republic Act No. 7722, Higher Education Act of 1994 (1994) (Philippines).
27) Republic Act No. 8293, Intellectual Property Code of the Philippines (1997) (Philippines).
28) Republic Act No. 10173, Data Privacy Act of 2012 (2012) (Philippines).

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: Edgardo C. Cagalitan