

Secure Digital Access Control for Technology-Enabled Learning in Vocational Education: A Qualitative Study of Stakeholder Perspectives

Kennedy Barfi Yaw Agyeibi^{1*}, Budi Mulyanti², Dwi Fitria Al Husaeni^{1,5}, Lala Septem Riza³,
Ilhamdaniah⁴

¹Technology and Vocational Education, School of Postgraduate Studies, Universitas Pendidikan Indonesia, Bandung, Indonesia

²Electrical Engineering, Faculty of Engineering and Industry Education, Universitas Pendidikan Indonesia, Bandung, Indonesia

³Computer Science Education, Faculty of Mathematics and Natural Sciences Education, Universitas Pendidikan Indonesia, Bandung, Indonesia

⁴Architecture, Faculty of Engineering and Industry Education, Universitas Pendidikan Indonesia, Bandung, Indonesia

⁵Data Science, Informatics and Computer, Universitas Ekuitas Indonesia, Bandung, Indonesia

*Corresponding Author

DOI: <https://doi.org/10.47772/IJRISS.2026.100801065>

Received: 11 September 2026; Accepted: 16 September 2026; Published: 24 September 2026

ABSTRACT

The digital transformation of vocational education has intensified cybersecurity challenges, yet research in developing-country contexts remains limited. This qualitative study examines stakeholder perspectives on cybersecurity in technology-enabled learning at Universitas Pendidikan Indonesia. One Focus Group Discussion with twelve purposively selected participants representing lecturers, IT personnel, administrative staff, and students was conducted, and the data were analyzed thematically. Findings reveal multidimensional challenges involving technical vulnerabilities, including single-factor authentication and open-source platform risks; human factors, including credential sharing and limited security awareness; human resource constraints; and institutional barriers such as reactive policies and a blame culture. These challenges are compounded by diverse user populations, resource limitations, and industry partnerships characteristic of vocational education. Participants recommended two-factor authentication, stronger password policies, institutional account integration, early security awareness, and differentiated digital literacy training. The findings highlight the need to view security and usability as interdependent socio-technical concerns and provide practical recommendations for developing secure, inclusive, and sustainable digital access systems in vocational education.

Keyword: Cybersecurity, vocational education, technology-enabled learning, digital access control, two-factor authentication, stakeholder perspectives.

INTRODUCTION

The rapid expansion of technology-enabled learning (TEL) has increased the dependence of educational institutions on learning management systems (LMS), single sign-on (SSO) platforms, cloud-based services, virtual learning environments, and other digital technologies. These systems facilitate access to learning resources, support flexible teaching and learning, and enable interaction across institutional and physical

boundaries. However, increasing digital dependence also expands the potential attack surface of educational institutions and creates challenges involving authentication, unauthorized access, privacy, data protection, and continuity of digital services. Research on cybersecurity in educational environments has highlighted the growing complexity of protecting digitally mediated learning and the need to address technological, human, and organizational vulnerabilities together (Abd El-Latif *et al.*, 2023; Afolalu & Tsoeu, 2025; Dhingra *et al.*, 2024; Greco, 2025).

Cybersecurity challenges in education cannot be attributed solely to weaknesses in technological infrastructure. User behavior is an important component of the security environment because practices such as credential sharing, weak password management, failure to recognize phishing attempts, and inadequate security awareness can undermine technical safeguards (Daudi, 2024; Morice, 2023; Parsons *et al.*, 2017). Evidence from e-learning environments further indicates that cybersecurity awareness and information-security policies are associated with safer user behavior (Oroni *et al.*, 2025). This suggests that effective digital access protection requires institutions to consider not only which technical controls are deployed but also whether users understand, accept, and can practically comply with those controls.

These concerns are particularly important in vocational education, where TEL is embedded within practical, competency-based learning activities. Vocational education commonly involves diverse groups of students and instructors, practical and laboratory-based activities, specialized digital applications, and interaction with external industry environments. Users may differ substantially in their levels of digital competence, and such

differences can affect how they interact with institutional technologies and security procedures. Research has identified variation in the digital competence of vocational teachers and learners, highlighting the importance of considering user capability when implementing digital technologies (Cattaneo *et al.*, 2022; Habibi *et al.*, 2023). At the same time, the growing adoption of artificial intelligence and other emerging technologies is expanding the range and complexity of digital tools used within vocational education (Çela *et al.*, 2024; Prasetya *et al.*, 2025; Regula, 2025). Connections between vocational institutions and industry can further complicate digital access because students and instructors may need to use external or industry-specific applications with different authentication and security requirements (Zervas & Stiakakis, 2025).

A related challenge concerns the relationship between cybersecurity and usability. Stronger authentication and access controls can improve protection, but additional security requirements may increase the effort required from users. Password complexity, additional authentication steps, session controls, and account-recovery procedures can become barriers when they are poorly designed or inadequately supported. However, the relationship between security and usability should not be understood as an unavoidable conflict. The effect of a security measure may depend on users' digital competence, familiarity with the system, perceived risk, and the extent to which adequate support is provided. Research on digital literacy and technology acceptance indicates that users' technological capabilities influence how they interact with digital systems and whether they are willing and able to adopt them effectively (Habibi *et al.*, 2023; Kabakus *et al.*, 2025; Purwita *et al.*, 2025).

Technology acceptance research provides an additional perspective for understanding secure digital access. Traditional technology acceptance models emphasize factors such as perceived usefulness and perceived ease of use, but research in educational and emerging-technology contexts suggests that acceptance can also be influenced by individual characteristics and contextual conditions (Alabed & Servi, 2026; Xue *et al.*, 2026). In the context of cybersecurity, users may evaluate an authentication or access-control mechanism not only according to whether it is useful or easy to use, but also according to whether they perceive it as trustworthy, understandable, necessary, and compatible with their existing practices. Consequently, digital literacy and technology acceptance should be considered when designing security mechanisms for heterogeneous vocational education populations.

Cybersecurity is therefore appropriately understood as a socio-technical problem. Technical controls operate within social, organizational, and institutional environments that influence their implementation and effectiveness. Users interact with security mechanisms according to their knowledge, attitudes, routines, and practical needs, while institutions determine policies, responsibilities, resources, and procedures for managing

cybersecurity. A socio-technical perspective is consequently useful for examining how technological systems interact with human and organizational factors in educational environments (Nowak *et al.*, 2022). This perspective is particularly relevant in institutions where cybersecurity capacity is constrained by limited financial resources, shortages of specialist personnel, legacy systems, and competing institutional priorities.

Institutional governance represents another important dimension of secure digital access. Effective cybersecurity requires more than the existence of written policies; it requires leadership commitment, clearly defined responsibilities, adequate resources, enforcement mechanisms, and coordination among technical and non-technical stakeholders. Research on cybersecurity governance emphasizes the organizational complexity of cybersecurity and the need for coordinated institutional responses rather than reliance on technical departments alone (Carr & Lesniewska, 2020; Hoong & Rezania, 2024). Studies addressing cybersecurity in educational institutions similarly indicate the importance of institutional arrangements, policy implementation, and organizational responsibility in managing digital security (Dei *et al.*, 2024).

The vocational education context makes these governance requirements particularly significant. Institutions must balance cybersecurity with the practical need for students and instructors to access digital resources quickly and reliably. Security controls that are technically appropriate but difficult to use may interfere with practical learning activities, while insufficient controls may expose institutional and user data to unnecessary risks. Moreover, vocational institutions may need to support interaction with external industry systems, specialized applications, and technologies that change rapidly. The expansion of AI and other digital technologies in vocational education adds further requirements for institutional capacity, digital competence, and responsible technology use (Çela *et al.*, 2024; Prasetya *et al.*, 2025; Regula, 2025).

Although research on educational cybersecurity, digital literacy, technology acceptance, and cybersecurity governance has expanded, important gaps remain in understanding how these dimensions interact within vocational TEL environments. Much of the existing literature addresses individual components of the problem, such as cybersecurity awareness, technology acceptance, digital competence, or institutional governance. Less attention has been given to how technical access-control mechanisms, user practices, human resource capacity, institutional governance, and the operational characteristics of vocational education interact from the perspectives of different stakeholder groups. This gap is particularly relevant in developing-country contexts, where resource limitations and institutional diversity may influence the feasibility of implementing sophisticated security mechanisms.

The present study addresses this gap through a qualitative investigation at Universitas Pendidikan Indonesia (UPI), Indonesia. It examines the perspectives of lecturers, IT personnel, administrative staff, and students who interact with institutional digital learning systems. The study focuses on three interconnected concerns: the security challenges experienced in digital access, practices that could support secure and usable access, and measures required to sustain and scale cybersecurity within vocational education. By bringing together technical, human, and institutional perspectives, the study seeks to provide empirical evidence for the development of secure digital access systems that are appropriate for the practical and organizational conditions of vocational TEL.

The study addresses the following research questions:

1. What are the key security challenges associated with digital access in vocational education?
2. What are the best practices for developing secure and user-friendly digital access systems for vocational education institutions?
3. What recommendations can be derived for sustaining and scaling digital security in vocational education?

The contribution of this study is threefold. First, it provides empirical evidence of cybersecurity challenges from multiple stakeholder perspectives within a vocational education setting. Second, it demonstrates that secure digital access should be considered through an integrated socio-technical lens that connects technical controls with user capability, usability, institutional governance, and vocational requirements. Third, it identifies practical measures for strengthening authentication, security awareness, digital literacy, human resource capacity, governance, infrastructure resilience, and user-centered system development. These findings

provide a basis for subsequent development of secure digital access-control solutions tailored to technology-enabled vocational learning environments.

METHODS

2.1. Research Procedures

This study employed a qualitative research design using a Focus Group Discussion (FGD) to investigate stakeholder perspectives concerning cybersecurity and digital access in vocational TEL. The FGD approach was selected because group interaction enables participants to build upon one another's experiences, challenge assumptions, and identify shared and divergent understandings of institutional practices (Krueger & Casey, 2014; Morgan, 1997). The approach was particularly suitable because the study brought together participants who interact with TEL systems from different institutional positions.

The FGD formed part of a broader research programme on secure digital access control for vocational TEL and served as a needs-analysis stage preceding subsequent system design and prototyping activities. The study was conducted at Universitas Pendidikan Indonesia (UPI), with the Faculty of Technology and Vocational Education as the principal institutional context. The purposive sampling strategy was intended to obtain information-rich perspectives from stakeholders whose roles gave them direct experience of learning, administrative, infrastructure, or security-related digital systems. Selection was consequently based on relevance to the study questions rather than statistical representativeness.

Purposive sampling was used to identify participants with direct experience of institutional TEL systems and perspectives relevant to cybersecurity. Inclusion criteria included current UPI affiliation, regular use of institutional LMS, SSO, or administrative platforms, a role relevant to cybersecurity or digital access, and willingness to participate and consent to audio recording. Twelve participants were selected: three lecturers, three IT personnel, one administrative staff member, and five students at undergraduate, master's, and doctoral levels. The participant profile and individual TEL-system experience are reported in Appendix B. This composition was intended to capture perspectives from direct learning-system users as well as personnel involved in technical and administrative functions.

The FGD lasted approximately 150 minutes and was conducted primarily in Indonesian to facilitate natural expression. The discussion followed the semi-structured guide in Appendix A, moving from participants' roles and current access-control mechanisms to security and privacy problems, characteristics of an ideal secure system, security-usability considerations, implementation barriers, user support and training, institutional policies, and recommendations. Open-ended questions were supplemented by follow-up probes where clarification or elaboration was needed. The session was audio-recorded with written consent, transcribed verbatim, reviewed against the recording, and anonymized through the use of participant codes P-A to P-L.

2.2 Instruments

The principal instrument was a semi-structured FGD guide comprising open-ended questions and follow-up probes concerning current access-control mechanisms, security and privacy problems, characteristics of an ideal secure system, security-usability considerations, implementation challenges, user support and training, policy recommendations and possible future participation in design or pilot activities. The sequence was designed to move from participants' experiences of existing systems toward desired characteristics and institutional recommendations. Audio recording and researcher observation notes were used to support data collection. The complete discussion guide is provided in Appendix A.

2.3 Data Analysis

The data were analyzed using thematic analysis following the six phases proposed by Braun and Clarke (2006). The researcher first became familiar with the transcripts and recordings, generated initial codes manually using Microsoft Excel, and subsequently grouped related codes into candidate themes. Candidate

themes were reviewed against coded extracts and the dataset as a whole, refined to ensure internal coherence and distinction from other themes, and then named, and interpreted in relation to the research questions and relevant literature. The analysis incorporated inductive patterns emerging from the data while also considering the study's research questions and conceptual concerns. The final analysis organized the findings around five interconnected dimensions rather than treating technical, human, and institutional issues as independent categories.

Analytical rigor was strengthened through independent review of a subset of the transcript by a second researcher, with differences discussed and resolved through consensus. Following preliminary analysis, a summary of findings was shared with participants; six participants provided feedback confirming the interpretation, with minor refinements incorporated. Analysis was conducted in Indonesian, while selected quotations were translated into English through translation, back-translation, and reconciliation.

2.4. Trustworthiness and Rigor

Several procedures were used to strengthen credibility, dependability, and confirmability. Credibility was supported by prolonged engagement with the audio recordings and verbatim transcripts, systematic thematic analysis, independent review of a transcript subset by a second researcher, and participant feedback on the preliminary interpretation. The latter involved six participants and resulted in minor refinements. Dependability was addressed through a clearly defined sequence of data preparation, coding, theme development, review, refinement, and interpretation, with coding maintained in Microsoft Excel and disagreements discussed to consensus. Confirmability was strengthened by grounding interpretations in the transcript data, retaining researcher observation notes, using participant codes rather than names, and subjecting part of the analysis to independent review. The study also reports the participant composition and institutional context in sufficient detail to support assessment of the applicability of the findings to other settings.

The analysis was conducted across the FGD dataset rather than as a formal comparison of stakeholder subgroups. Accordingly, the findings are presented primarily as themes shared or discussed across the group. The participant profile nevertheless provides contextual differentiation: lecturers and students represented direct learning-system use, IT personnel represented infrastructure and system-administration functions, and the administrative staff member represented administrative-system use. Because the study was based on a single FGD and was not designed to estimate subgroup-level differences, these role distinctions are used to contextualize the findings rather than to claim systematic differences between stakeholder groups.

2.4. Ethical Considerations

Ethics approval for this study was obtained before data collection from the relevant institutional ethics review body, the Ethics Commission of the Universitas Pendidikan Indonesia, Bandung, Indonesia, with approval reference number No.255/UN40.K/PT.01.01/2025. This study was conducted in accordance with established ethical principles for research involving human participants, including respect for autonomy, voluntary participation, confidentiality, anonymity, and secure data management. Confidentiality was maintained through pseudonyms, removal of identifying information, password-protected data storage, and aggregated reporting where possible. Audio recordings, transcripts, and associated research materials were handled as confidential study data, with participant identifiers replaced by codes P-A to P-L.

RESULTS AND DISCUSSION

The analysis produced five interconnected dimensions of cybersecurity challenges: technical vulnerabilities, user behavior, human resource constraints, institutional barriers, and vocational education-specific conditions. The findings also indicate that participants understood secure digital access as a combination of technical protection, usability, user capability, institutional governance, and organizational support. This integrated pattern is consistent with a socio-technical interpretation of cybersecurity in which security emerges through

interactions between technological systems, people, and organizational structures (Nowak *et al.*, 2022).

The stakeholder composition provides useful context for interpreting these themes. The dataset included three lecturers and five students who regularly used learning or academic systems, three IT personnel with infrastructure or system-administration responsibilities, and one administrative staff member who used an administrative system. The study did not treat these categories as independent analytical samples; instead, their inclusion was intended to bring different forms of institutional experience into the same discussion. Consequently, the findings below should be read as an integrated account of the FGD rather than as evidence that one stakeholder group experienced a particular challenge more frequently than another.

3.1. What are the key security challenges associated with digital access in vocational education?

Technical vulnerabilities

Participants identified authentication and access control as major technical concerns. The absence of multi-factor authentication was viewed as a significant weakness, while password-based authentication was considered vulnerable to guessing, theft, and sharing. Although SSO was valued for convenience, participants also recognized that compromise of a single institutional account could affect access to multiple services. Participants further reported inconsistent access-control practices across institutional systems and expressed concerns about open-source platforms when configuration and maintenance were inadequate.

These findings indicate that the challenge is not simply the absence of a particular security technology but the relationship between existing technical architecture and institutional capacity. Research on cybersecurity in education similarly emphasizes the need to address authentication, access protection, data security, and organizational preparedness together (Abd El-Latif *et al.*, 2023; Afolalu & Tsoeu, 2025; Greco, 2025). The participants' concerns therefore suggest that introducing stronger authentication should form part of a broader access-control strategy rather than be treated as an isolated technical intervention.

The findings concerning open-source platforms also require contextual interpretation. Open-source technology can provide institutions with flexibility and potentially lower acquisition costs, but its security depends on appropriate configuration, maintenance, updating, and institutional oversight. The relevant issue is consequently not whether software is open source itself, but whether the institution possesses the capacity to manage the security of the technologies it deploys.

User behavior and security awareness

User behavior emerged as another important source of vulnerability. Participants reported credential sharing, weak security practices, and phishing experiences involving students and lecturers. Credential sharing was partly associated with difficulties maintaining access when systems were unavailable or inconvenient. Participants also indicated that some users did not fully understand the consequences of insecure practices.

This finding is consistent with research emphasizing the human dimensions of cybersecurity. Security behavior is influenced by users' perceptions, trust, awareness, and practical circumstances (Daudi, 2024; Morice, 2023). Parsons *et al.* (2017) likewise demonstrate the importance of human aspects in information-security behavior. The present findings extend this perspective by showing that insecure behavior within vocational TEL may be partly shaped by the accessibility and reliability of the systems themselves. When legitimate access is difficult, users may adopt informal practices to maintain continuity.

The implication is important for system design. Security awareness programmes should not simply instruct users to comply with security rules. Institutions should also examine whether technical and organizational arrangements unintentionally encourage insecure workarounds. Oroni *et al.* (2025) similarly highlight the relationship between cyber awareness, information-security policies, and safer behavior among e-learning students.

Human resource constraints

Participants described difficulties recruiting and retaining qualified cybersecurity personnel, with external employment perceived as more financially attractive. The shortage of personnel was considered to constrain cybersecurity management, technical support, and system improvement. Participants also referred to the absence of a fully operational CSIRT despite regulatory expectations.

This finding demonstrates that cybersecurity capacity is partly a workforce problem. Institutions may recognize technical weaknesses and understand the need for stronger controls but remain unable to implement improvements because the necessary expertise and staffing are unavailable. Calderaro & Craig (2020) similarly identify unequal cybersecurity capacity as an important governance challenge, particularly where institutional and national resources for cyber capacity building differ.

The implication is that security strategies developed without considering workforce capacity may be difficult to sustain. Cybersecurity investment should therefore include recruitment, retention, professional development, incident-response capability, and appropriate allocation of responsibilities.

Institutional barriers and organizational culture

Participants described security policy development as predominantly reactive, with changes sometimes occurring after security incidents. They also reported organizational dynamics in which IT personnel could be held responsible for incidents even when the underlying application or system was developed elsewhere. Such conditions were perceived as discouraging open reporting and proactive security improvement.

These findings reinforce the view that cybersecurity is an institutional governance issue. Organizational responsibilities, decision-making processes, accountability structures, and leadership influence whether security risks are addressed proactively. Cybersecurity governance research similarly emphasizes the interaction between technical concerns and organizational structures (Carr & Lesniewska, 2020; Hoong & Rezania, 2024).

The reported blame culture is particularly significant because security improvement depends on the willingness of staff to identify and communicate vulnerabilities. A culture that primarily assigns blame after an incident may reduce incentives for early reporting. Thus, strengthening cybersecurity requires not only policies and technical controls but also an organizational environment in which security concerns can be reported and addressed constructively.

Vocational education-specific conditions

Participants identified several conditions that distinguish vocational education from more conventional educational environments. These included diverse user populations, differences in digital literacy, limited resources, and the need to integrate institutional systems with industry software. Participants specifically emphasized that industry applications may operate under different security requirements and that security education should be relevant to students' future workplaces.

This finding corresponds with evidence that digital competence varies among vocational teachers and learners (Cattaneo *et al.*, 2022; Habibi *et al.*, 2023). The expansion of AI and other digital technologies within vocational education further increases the range of systems and skills that institutions must manage (Çela *et al.*, 2024; Prasetya *et al.*, 2025; Regula, 2025).

This demonstrates that cybersecurity challenges in vocational TEL cannot be reduced to inadequate technical controls. They arise from the interaction of technical weaknesses, user practices, human resource limitations, institutional governance, and the distinctive operational conditions of vocational education. This provides empirical support for treating secure digital access as a socio-technical rather than exclusively technological problem.

3.2. What are the best practices for developing secure and user-friendly digital access systems for vocational education institutions?

Stronger authentication and access control

Participants strongly supported two-factor authentication as a means of strengthening digital access. They also recommended mandatory password policies, continued use of session-management controls such as automatic logout, and integration of institutional accounts across digital services. Institutional account integration was valued because it could support policy enforcement, monitoring, and account deactivation when necessary.

These findings indicate that participants did not reject stronger security controls because of usability concerns. Instead, they expected security mechanisms to be implemented in ways that remained manageable for users. This is important because research on educational cybersecurity identifies authentication and policy enforcement as central components of protecting digital learning environments (Abd El-Latif *et al.*, 2023; Greco, 2025).

The findings also suggest that centralized institutional identity management can provide both security and administrative benefits. However, because SSO may concentrate access privileges, institutional account integration should be accompanied by appropriate authentication, monitoring, session management, and recovery procedures.

Security policies and early socialization

Participants recommended comprehensive and accessible guidelines covering LMS use, SSO accounts, learning activities, and account security. They also supported clear rules and sanctions concerning IT or account misuse. Security awareness was viewed as something that should be introduced during student orientation and other early institutional activities rather than after users had already developed insecure practices.

This finding is consistent with evidence that cybersecurity awareness and information-security policies are important components of safer e-learning behavior (Oroni *et al.*, 2025). It also reinforces the governance literature, which emphasizes that cybersecurity requires clear institutional responsibilities and policies rather than reliance on individual users alone (Dei *et al.*, 2024).

Importantly, participants linked rules with individual responsibility and ethical behavior. This suggests that sanctions should not function solely as punitive mechanisms. They should be accompanied by clear communication, education, and support so that users understand both the rationale for the rules and the consequences of non-compliance.

User support, digital literacy, and mentoring

Participants recommended increasing IT staffing, improving system user guides, providing mentoring, and delivering continuous digital literacy training. Particular attention was given to users with lower levels of technological familiarity. Participants emphasized that training should continue beyond initial orientation.

This finding is consistent with research linking digital competence and technology acceptance. Differences in digital literacy can affect users' ability to engage effectively with technology (Habibi *et al.*, 2023; Kabakus *et al.*, 2025; Purwita *et al.*, 2025). In vocational environments, where user capabilities can vary substantially, differentiated support may therefore be more appropriate than a uniform training programme.

The findings also suggest that digital literacy should be understood as an ongoing institutional capability rather than a one-time training outcome. Security threats and digital systems change over time, requiring continuous learning and reinforcement.

User-centered development

Participants emphasized that secure systems should be developed through adequate research, prototyping, and feedback from actual users. They associated insufficient user feedback with systems that were less intuitive.

This finding is particularly important to the security-usability relationship. Rather than treating usability as an additional feature evaluated after security controls have been implemented, participants viewed user involvement as part of the development process itself. This position is consistent with the broader technology-acceptance literature, which recognizes the importance of user characteristics and contextual factors in technology adoption (Alabed & Servi, 2026; Xue *et al.*, 2026).

The findings also refine the interpretation of the security-usability trade-off. The burden imposed by a security measure is not necessarily the same for every user. A mechanism that is straightforward for a digitally experienced student may be more difficult for a lecturer or staff member with lower digital confidence. Consequently, usable security should be designed around the characteristics of the actual user population.

This indicates that secure and user-friendly digital access requires a combination of technical controls, institutional identity management, clear policies, user education, continuous support, and participatory development. No single control is sufficient on its own.

3.3. What recommendations can be derived for sustaining and scaling digital security in vocational education?

Human resource development

Participants identified human resource development as a central requirement for sustainability. They recommended increasing IT personnel and ensuring that staff possess appropriate technical competencies.

This finding demonstrates that the sustainability of security controls depends on the institution's capacity to maintain them. Technical systems require monitoring, maintenance, incident response, updates, and user support. Without sufficient personnel, even appropriate security measures may deteriorate over time. The finding is therefore consistent with broader concerns about uneven cybersecurity capacity and workforce limitations (Calderaro & Craig, 2020).

Policy development and enforcement

Participants recommended clear and accessible policies covering LMS use, SSO accounts, learning activities, and IT or account misuse. They also supported rules and sanctions and the integration of security awareness into student orientation.

These recommendations reinforce the governance dimension identified under RQ1. Sustainability requires a shift from reactive policy development toward continuous institutional risk management. Governance mechanisms should clearly define responsibilities across IT, academic units, administrators, and users rather than placing cybersecurity responsibility exclusively on technical personnel.

This is consistent with the broader literature, which conceptualizes cybersecurity governance as a collective institutional responsibility involving policy, organizational structures, accountability, and coordination (Carr & Lesniewska, 2020; Dei *et al.*, 2024; Hoong & Rezania, 2024).

Continuous training and user support

Participants emphasized that digital literacy training should be ongoing rather than limited to orientation and recommended mentoring for users who require additional support.

This recommendation is particularly relevant given the diversity of users identified in the study. Digital

competence is not static, and the introduction of new technologies can create new learning requirements. Research on digital literacy and technology acceptance similarly indicates that users' capabilities influence their engagement with digital technologies (Cattaneo *et al.*, 2022; Habibi *et al.*, 2023; Kabakus *et al.*, 2025).

A sustainable security strategy should therefore incorporate recurring awareness activities, practical guidance, mentoring, and mechanisms through which users can obtain assistance when security controls interfere with their learning or work.

Infrastructure resilience and scalability

Participants viewed existing data redundancy and backup arrangements positively and emphasized the need for scalable architecture capable of supporting increasing numbers of users and applications.

These findings indicate that sustainability involves both security and continuity. In TEL environments, system availability is important because interruptions can affect teaching, assessment, practical activities, and access to learning resources. Resilient infrastructure, redundancy, backup arrangements, and scalable architecture should therefore be incorporated into digital access planning rather than addressed only after failures occur.

Institutional culture and leadership

Participants emphasized collaboration between IT and other institutional units and called for leadership support through appropriate resource allocation and prioritization of cybersecurity.

This finding reinforces the socio-technical interpretation developed throughout the study. Cybersecurity cannot be sustained by an IT department operating independently from academic and administrative units. Leadership determines whether cybersecurity receives adequate resources, whether responsibilities are clearly assigned, and whether security is incorporated into institutional decision-making.

The finding is also consistent with research that treats cybersecurity governance as an organizational problem requiring coordination among multiple stakeholders (Carr & Lesniewska, 2020).

Vocational and industry-specific considerations

Finally, participants emphasized that security measures should reflect the practical nature of vocational education. Security training should be relevant to students' future workplaces, while institutional systems should be able to interact securely with industry software that may operate under different security requirements.

This requirement distinguishes vocational TEL from more general educational environments. Vocational learning frequently involves practical technologies and external systems, making secure interoperability an important design consideration. The growing use of AI and emerging technologies in vocational education further increases the need for context-sensitive security practices (Çela *et al.*, 2024; Regula, 2025; Zervas & Stiakakis, 2025).

Taken together, research question 3 demonstrates that sustaining and scaling digital security requires simultaneous investment in technical infrastructure, human resources, governance, user capability, organizational culture, and industry integration. Security should therefore be treated as an institutional capability that develops over time rather than as a one-time technology implementation.

Integrated interpretation

Across the three research questions, the findings reveal a consistent pattern. First, security weaknesses are produced through interactions among technical architecture, user behavior, institutional resources, and governance. Second, participants did not perceive security and usability as mutually exclusive objectives; rather, they expected security controls to be adapted to users' capabilities and supported by training and accessible design. Third, long-term security depends on institutional capacity, including adequate personnel,

policies, leadership, infrastructure, and continuous learning.

The findings provide preliminary support for extending conventional technology-acceptance perspectives in security contexts. Participants' willingness to accept stronger authentication despite anticipated inconvenience suggests that security acceptance may involve considerations related to perceived risk, trust, responsibility, digital competence, and contextual circumstances in addition to perceived usefulness and ease of use. Existing research demonstrates that technology acceptance in education is influenced by individual and contextual characteristics (Alabed & Servi, 2026; Kabakus *et al.*, 2025; Xue *et al.*, 2026). The present findings suggest that these factors warrant more explicit consideration when the technology being accepted is itself a security mechanism.

The findings also reinforce a socio-technical understanding of cybersecurity. Technical safeguards cannot be separated from organizational practices, user behavior, institutional culture, and governance. The reported interaction among inadequate authentication, credential sharing, staffing shortages, reactive policy development, and differences in digital competence illustrates how vulnerabilities can accumulate across multiple layers of an institution (Nowak *et al.*, 2022).

Practical implications

For institutions, the findings support prioritizing stronger authentication for institutional accounts, strengthening password and session-management practices, improving identity management, developing accessible security guidelines, increasing cybersecurity staffing, and providing continuous digital literacy support. Developers should incorporate user research, prototyping, and stakeholder feedback throughout system development. For policymakers and institutional leaders, cybersecurity requirements should be accompanied by realistic implementation support, particularly where vocational institutions face resource constraints.

The practical implication is not that every vocational institution should adopt the same technical architecture. Instead, institutions should establish a baseline of secure access controls and adapt implementation to their users, infrastructure, governance arrangements, and relationships with industry. Such an approach is more consistent with the socio-technical nature of cybersecurity and with the diversity of vocational education environments.

LIMITATIONS AND FUTURE RESEARCH

Several limitations should be considered when interpreting the findings. The study was conducted at a single institution and therefore does not establish that the identified conditions are representative of all vocational education institutions. Transferability is consequently limited and depends on the extent to which other institutions share comparable TEL infrastructure, governance arrangements, user diversity, and resource conditions. The use of one FGD with 12 participants may also have limited the range of perspectives captured, while the presence of participants from different institutional roles may have influenced the openness of discussion. Although the participant composition included lecturers, students, IT personnel, and administrative staff, the analysis was not designed as a formal comparison of stakeholder subgroups; the study therefore cannot establish systematic differences between these groups. The cross-sectional design captures perceptions at one point in time, and self-reported accounts may be affected by recall or social desirability. Researcher positionality and translation from Indonesian into English may also have influenced interpretation.

Future research should therefore examine secure digital access across multiple vocational institutions and, where appropriate, across countries. Larger and more diverse samples could provide stronger evidence concerning differences among students, lecturers, administrators, and IT personnel, while separate interviews or FGDs could allow stakeholder-specific experiences to be examined without the interaction effects of a mixed-role group. Longitudinal research could assess whether proposed security interventions produce sustained improvements in security behavior and user acceptance. Future studies should also triangulate stakeholder accounts with system logs, incident reports, policy documents, and other institutional records. Further research could examine security-specific extensions of technology-acceptance models and investigate

whether age, digital literacy, prior experience, and other user characteristics moderate perceptions of security measures. Participatory design research could additionally involve stakeholders directly in developing and evaluating secure access-control interventions.

CONCLUSION

This study examined stakeholder perspectives on cybersecurity and secure digital access within technology-enabled vocational education at Universitas Pendidikan Indonesia. The findings demonstrate that cybersecurity challenges are multidimensional, involving technical vulnerabilities, insecure user behavior, limited cybersecurity personnel, reactive governance, organizational culture, diverse user capabilities, resource constraints, and the complexity of integrating institutional and industry systems. Participants supported stronger authentication, institutional account integration, effective session management, clear security policies, early security awareness, continuous and differentiated digital literacy support, and user-centered system development. The findings further indicate that the security-usability relationship depends partly on user characteristics and that secure digital access should be understood as a socio-technical institutional capability. These conclusions are grounded in one institutional case and should consequently be considered in relation to the contextual conditions of UPI and similar vocational education settings.

Sustaining and scaling cybersecurity in vocational education requires coordinated technical, human, and organizational action. Institutions need adequate cybersecurity personnel, proactive governance, clear policies and enforcement mechanisms, continuous user support, resilient infrastructure, and leadership commitment. Developers should incorporate user diversity and vocational learning requirements into system design, while institutional leaders and policymakers should ensure that security expectations are supported by realistic resources and implementation mechanisms. Overall, secure digital access in vocational education cannot be achieved through technical controls alone; it requires alignment among technology, users, institutional governance, and the practical conditions in which vocational learning occurs.

ACKNOWLEDGMENT

The authors thank the participants for their valuable contributions to this study. This research was conducted as part of a doctoral dissertation at Universitas Pendidikan Indonesia. Special appreciation is extended to the Faculty of Technology and Vocational Education for facilitating this research.

AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. The authors confirmed that the paper was free of plagiarism.

REFERENCES

1. Abd El-Latif, A., Yassine, M., Elaffendi, M., & Ahmad, S. (2023). Cybersecurity Management in Education Technologies: Risks and Countermeasures for Advancements in E-learning. <https://doi.org/10.1201/9781003369042>
2. Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. *Future Internet*, 17(12), 575. <https://doi.org/10.3390/fi17120575>
3. Alabed, T., & Servi, S. (2026). Profiling Teachers' Technology Acceptance and Digital Competence Using Machine Learning Techniques. *Turkish Journal of Mathematics and Computer Science*, 18(1), 126–142. Scopus. <https://doi.org/10.47000/tjmcs.1778991>
4. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
5. Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), 917–938. <https://doi.org/10.1080/01436597.2020.1729729>

6. Carr, M., & Lesniewska, F. (2020). Internet of Things, cybersecurity and governing wicked problems: Learning from climate change governance. *International Relations*, 34(3), 391–412. Scopus. <https://doi.org/10.1177/0047117820948247>
7. Cattaneo, A. A. P., Antonietti, C., & Rauseo, M. (2022). How digitalised are vocational teachers? Assessing digital competence in vocational education and looking at its underlying factors. *Computers and Education*, 176. Scopus. <https://doi.org/10.1016/j.compedu.2021.104358>
8. Çela, E., Vajjhala, N. R., Potluri, R. M., & Eappen, P. (2024). Transforming Vocational Education and Training Using AI. In <https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/979-8-3693-8252-3>. IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-8252-3>
9. Daudi, M. (2024). Exploiting Human Trust in Cybersecurity: Which Trust Development Process is Predominant in Phishing Attacks? *Applied Cybersecurity and Internet Governance*, 3(2), 233–249. Scopus. <https://doi.org/10.60097/ACIG/199452>
10. Dei, H., Shvets, D., Lytvyn, N., Sytnichenko, O., & Kobus, O. (2024). Legal Challenges and Perspectives of Cybersecurity in the System of State Governance of Educational Institutions in Ukraine. *Journal of Cyber Security and Mobility*, 13(5), 963–982. Scopus. <https://doi.org/10.13052/jcsm2245-1439.1357>
11. Dhingra, M., Goyal, R., & Goyal, S. J. (2024). Cybersecurity Challenges and Opportunities in Education 4.0. In S. A. Abdul Karim (Ed.), *Intelligent Systems Modeling and Simulation III: Artificial Intelligent, Machine Learning, Intelligent Functions and Cyber Security* (pp. 333–342). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-67317-7_20
12. Greco, D. (2025). Security in E-Learning: A Systematic Review. In M. Ruo Roch, F. Bellotti, R. Berta, M. Martina, & P. Motto Ros (Eds), *Applications in Electronics Pervading Industry, Environment and Society* (pp. 457–465). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-84100-2_54
13. Habibi, A., Sofyan, S., & Mukminin, A. (2023). Factors affecting digital technology access in vocational education. *Scientific Reports*, 13(1), 5682.
14. Hoong, Y., & Rezania, D. (2024). Navigating Cybersecurity Governance: The influence of opportunity structures in socio-technical transitions for small and medium enterprises. *Computers and Security*, 142. Scopus. <https://doi.org/10.1016/j.cose.2024.103852>
15. Kabakus, A. K., Bahcekapili, E., & Ayaz, A. (2025). The effect of digital literacy on technology acceptance: An evaluation on administrative staff in higher education. *Journal of Information Science*, 51(4), 930–941. Scopus. <https://doi.org/10.1177/01655515231160028>
16. Krueger, R. A., & Casey, M. A. (2014, July). *Focus Groups: A practical guide for applied research*. SAGE Publications Ltd. <https://uk.sagepub.com/en-gb/asi/focus-groups/book243860>
17. Morgan, D. L. (1997). *Focus groups as qualitative research* (2nd ed). Sage Publications.
18. Morice, D. (2023). Trust Framework on Exploitation of Humans as the Weakest Link in Cybersecurity. *Applied Cybersecurity and Internet Governance*, 2(1), 179–204. Scopus. <https://doi.org/10.60097/ACIG/162867>
19. Nowak, V., Ullrich, J., & Weippl, E. (2022). Cybersecurity is more than a Technological Matter – Towards Considering Critical Infrastructures as Socio-Technical Systems. *Applied Cybersecurity and Internet Governance*, 1(1). Scopus. <https://doi.org/10.5604/01.3001.0016.2055>
20. Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025). Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis. *Computers & Security*, 150, 104276.
21. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40–51. <https://doi.org/10.1016/j.cose.2017.01.004>
22. Prasetya, F., Fortuna, A., Samala, A. D., Latifa, D. K., Andriani, W., Gusti, U. A., Raihan, M., Criollo-C, S., Kaya, D., & Cabanillas García, J. L. (2025). Harnessing artificial intelligence to revolutionize vocational education: Emerging trends, challenges, and contributions to SDGs 2030. *Social Sciences & Humanities Open*, 11, 101401. <https://doi.org/10.1016/j.ssaho.2025.101401>
23. Purwita, A. W., Elfaiz, E. A., & Rahmaningrum, A. (2025). Teachers and Technology Acceptance: The Role of Digital Literacy, Technology Anxiety, and Cognitive Perceptions in Prediction Behavioral Intention. *Proc. - Int. Conf. Inf. Technol., Inf. Syst. Electr. Eng., ICITISEE*, 66–71. Scopus. <https://doi.org/10.1109/ICITISEE68184.2025.11355052>

24. Regula, K. C. (2025). AI and Cybersecurity: A Symbiotic Relationship for Sustainable Technical and Vocational Education. In A. Sorayyaei Azar, S. Kant Gupta, H. Taherdoost, & F. Alhamaty (Eds), *Advances in Computational Intelligence and Robotics* (pp. 299–318). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3373-1142-5.ch015>
25. Xue, L., Mahat, J., & Ghazali, N. (2026). Technology Acceptance Model in Artificial Intelligence in Education: A Meta-Analysis. *Sage Open*, 16(1), 21582440251409441. <https://doi.org/10.1177/21582440251409441>
26. Zervas, I., & Stiakakis, E. (2025). Emerging Digital Skills in Vocational Education: The Impact of AI on Laboratory-Based Learning. *EDULEARN25 Proceedings*, 2772–2782. 17th International Conference on Education and New Learning Technologies. <https://doi.org/10.21125/edulearn.2025.0776>

APPENDICES

Appendix A

FGD Discussion Guide

The following questions guided the Focus Group Discussion:

1. Can you briefly introduce yourself and describe your role at the institution?
2. What types of access control mechanisms are currently used in your TEL systems?
3. What security or privacy issues have you or your institution encountered?
4. What would an ideal secure access control system look like in your setting?
5. How do you perceive the balance between system security and ease of access?
6. What are the biggest challenges to implementing secure digital access in VET?
7. How should institutions support users (teachers, students) in using secure systems?
8. What policies or practices are needed to ensure the responsible use of TEL platforms?
9. What final recommendations do you have for improving secure access control in TEL?
10. Would you be open to participating in a design workshop or pilot?

Appendix B

Participant Demographics

Participant	Role	Affiliation	Academic Level	Experience with TEL Systems
P-A	Lecturer	Technical and Vocational Education; Culinary Education - FPTI	Professor	Regular user of LMS, SSO, VPN
P-B	IT Administrator; Doctoral Student	TVE; Infrastructure and Application Development	Doctoral	System administrator, developer
P-C	Doctoral Student	TVE	Doctoral	Regular user of research and academic systems
P-D	Master's Student	TVE	Master's	Student user of LMS,

				SSO
P-E	Master's Student	TVE	Master's	Student user of academic systems
P-F	Undergraduate Student	Family Welfare Education - FPTI	Undergraduate	Student user of LMS, SSO
P-G	Doctoral Student	TVE	Doctoral	Research system user
P-H	Lecturer	Family Welfare Education	Professor	Regular user of LMS, SSO
P-I	Lecturer	Electrical Engineering Education	Professor	Regular user of LMS, SSO, lab systems
P-J	Administrative Staff	Architecture Engineering Education	Undergraduate	Administrative system user
P-K	Network Administrator	ICT Directorate	Master's	Network infrastructure management
P-L	Systems Administrator	ICT Directorate	Master's	System administration and security