

2025 EDUCAUSE Horizon Action Plan: Supporting Agency, Trust, Transparency, and Involvement

Jenay Robert



EDUCAUSE

2025 EDUCAUSE Horizon Action Plan: Supporting Agency, Trust, Transparency, and Involvement

Jenay Robert, *2025 EDUCAUSE Horizon Action Plan: Supporting Agency, Trust, Transparency, and Involvement* (Boulder, CO: EDUCAUSE, 2025)

© 2025 EDUCAUSE

This report is licensed under the [Creative Commons BY-NC-ND 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Learn More

Read additional materials on the research hub for the [2024 EDUCAUSE Horizon Report: Cybersecurity and Privacy Edition](#).

EDUCAUSE

EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision-making at every level within higher education. EDUCAUSE is a global nonprofit organization whose members include U.S. and international higher education institutions, corporations, not-for-profit organizations, and K-12 institutions. With a community of more than 100,000 individuals at member organizations located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation. For more information, please visit edUCAUSE.edu.

In the [2024 EDUCAUSE Horizon Report: Cybersecurity and Privacy Edition](#), a panel of experts agreed that a key practice for advancing the future of higher education cybersecurity and privacy is supporting agency, trust, transparency, and involvement among stakeholders. In fact, these are such important topics for the higher education community that “restoring trust” surfaced as the overarching theme for the [2025 EDUCAUSE Top 10](#), and issue number four is “[A Matter of Trust: Advancing institutional strategies to safeguard privacy and secure institutional data](#).” In an increasingly unpredictable world, an imperative for higher education is shoring up the most foundational cybersecurity and privacy practices: honoring end users’ agency, fostering trust both within the academic community and beyond, centering transparency to the highest extent possible, and involving all stakeholders in the daily work and responsibility of cybersecurity and privacy.

Our expert panel was charged with envisioning the preferred future of supporting agency, trust, transparency, and involvement in higher education and creating an action plan toward that future. Panelists were asked to focus on a 10-year time horizon, which allows us to realistically consider the future impacts of current social, technological, economic, environmental, and political trends. **Keeping this time horizon in mind is important, given the volatility of many of the social, technological, economic, environmental, and political trends, making it difficult to predict their evolution, especially in the immediate future.**

Building on the trends, technologies, practices, and scenarios described in the *2024 EDUCAUSE Horizon Report: Cybersecurity and Privacy Edition*, panelists collaboratively generated a description of their preferred future for higher education. Working backwards from this vision, the panel identified actions that individuals, departments, cross-department collaborators, and cross-institution collaborators can take to make that preferred future a reality.

Activity: Imagine Future You

Imagining the future can be challenging. Our daily lives require us to be present in the moment, considering threats and opportunities that exist around us. Take a minute to jump-start your creativity and foresight by answering the following questions.

- What will your life look like 10 years from today? Envision your home, hobbies, family, and friends.
- What will your work look like 10 years from today? Envision your work space, daily activities, and colleagues.

Contents

Goals for Our Future State	4
Actions	5
Planning for the Road Ahead	8
Methodology	10
Expert Panel Roster	11

GOALS FOR OUR FUTURE STATE

Asked to describe their preferred state of higher education 10 years from now, panelists collaboratively described the following:

Technology budgets have increased. Increasing student enrollments, coupled with increasing sophistication and integration of educational technology, have resulted in larger technology budgets across higher education. More budget is dedicated to resolving and avoiding technical debt.

Data governance is distributed and collaborative. IT units are not solely responsible for data ownership, so risk and compliance are shared across the institution. Data are unified across sources both within and between institutions to facilitate research and analytics. Use of data is responsible and ethical, and data subjects are informed about the collection and use of their data.

Data literacy programs support end users' understanding of cybersecurity and data privacy. End users—including students—have sufficient guidance to understand how to use and protect personal information, decreasing the threat of cybersecurity attacks and accidental exposure by insiders (i.e., insider threat).

Higher education institutions use a robust identity system architecture. Supported by concise federal policies and international standards, institutions center data privacy in daily operations. Institutions have strong security controls in place to safeguard data from unauthorized access or use.

Faculty, staff, and students use AI technologies ethically and responsibly. The proliferation of AI tools has increased institutions' need for defensive capabilities, but it has also expanded the ways in which AI can be used to commit cyberattacks.

Higher education institutions disincentivize ransomware attacks. All institutions have an international agreement to not pay cyber criminals who demand ransom.

A mix of remote and on-site operations is commonplace. Institutions offer a variety of modalities to meet the changing needs of students, faculty, and staff.

Institutions help end users protect intellectual property. Increasing threats to proprietary information, including research data, have necessitated an increased focus on protecting intellectual property.

The United States has adopted a national standard for cybersecurity and privacy. This national standard provides consistency in how higher education institutions operate, ensuring a robust security posture that mitigates the threat landscape.

Panelists generated a list of actions that individuals, units and departments, and multi-unit or multi-institutional teams can take to arrive at this preferred future in 10 years.

Individuals

Individual-level actions in higher education refer to efforts taken by individual faculty, staff, or students to contribute to shared institutional or collaborative goals.

Understand the importance of data privacy by seeking training for privacy champions and privacy liaisons.

When privacy starts with individuals, everyone wins. Individuals increase their agency by exercising their rights, and they also become more involved in institutional privacy functions.

Provide leadership to shift the cultural focus across the enterprise. Cultural change requires both top-down and bottom-up leadership. Involvement of leaders at all levels helps define the institution's stance on privacy and security, aligns efforts between institutional silos, and helps address the chronic underfunding of privacy and security functions.

Engage in best practices to protect intellectual property in the age of AI. As an example, avoid plagiarism by citing the use of AI technologies in academic, research, and operational activities. Seek training and other institutional supports to learn how AI models are trained and how to appropriately cite them. Individuals must understand the sensitivity of the data they share with any technology, including AI.

Units and Departments

Unit- and department-level actions refer to the collective efforts of functional units or departments (e.g., academic, administrative, and support) to contribute to shared institutional or collaborative goals.

Provide members of the unit or department with in-depth awareness training. This common piece of advice continues to be a high priority for privacy and security professionals. Unfortunately, many barriers stand in the way of creating and delivering effective training. For example, the higher education workforce as a whole often lacks the time or funding necessary to create or participate in additional work responsibilities.

Create accountability mechanisms for privacy and security policies. As an example, create consequences for individuals who do not complete training or who fail simulation tests. Creating such accountability mechanisms can be risky, though. Consequences that are too lenient will not produce the desired behavioral changes, and consequences that are too harsh can foster resentment. Work with HR and student policy units to navigate these issues.

Improve identity validation. Improved identity validation can help institutions reduce identity theft, decrease academic dishonesty, and build trust with stakeholders. Units and departments need to investigate new tools and models that support and enhance identity validation and employ skilled staff to help implement those tools and models.

Restrict the use of purchasing cards for technology that has not been vetted. This approach to procurement helps align with institutional processes for assessing information security, privacy, and data usage risks and reduces the risks associated with individual licensing.

Stay up-to-date on evolving security trends. Regularly implementing the most updated systems and applications improves compliance and decreases risk. Certainly, this is another action item that requires time, funding, and expertise—resources that may be in short supply at some institutions.

Multi-Unit Collaboration

Multi-unit collaboration refers to coordinated efforts between different departments, divisions, or units within an institution to achieve shared goals, solve complex challenges, or enhance services. This collaboration can include partnerships between academic departments, administrative offices, student support services, research centers, and other units, enabling the pooling of resources, expertise, and perspectives.

Improve needed infrastructure—not just student-facing technology. Focusing on infrastructure leads to more efficient use of IT resources. Working together across units helps institutions identify shared needs, identify and prioritize technical debt, and improve the value proposition for new infrastructure.

Adopt a risk-management framework in which departments and units are responsible for their own technology and data risks. Central IT and cybersecurity units should not own all technology risk for the organization; it needs to be owned and managed by the business units that rely on the technology. This structure reduces the adversarial relationship between units and central IT and empowers units to weigh risks effectively. Start with a common understanding of risk at an institutional scale to ensure that all stakeholders are on the same page.

Bring together stakeholders from across the institution to strategize, formulate, and implement AI governance. Collaborative strategies increase transparency around AI-related decision-making and enable the institution to be innovative in its use of technology. Be sure to include stakeholders from a wide range of departments and units, ensuring that more people have access to the technology and preventing silos.

Make cybersecurity, privacy, and data usage part of technology decisions before the procurement process. Including cybersecurity, privacy, and data usage considerations earlier in technology decisions helps end users understand that cybersecurity and privacy are not roadblocks.

Sponsor institution-wide learning events to generate new ideas and improve collaboration. Such events can increase stakeholder excitement, raise awareness, set clear expectations with end users, and generate new partnerships with IT. Take advantage of in-house expertise to refine training materials.

Engage students when implementing data security and privacy policies. Help students be involved in policy-making rather than having policies forced upon them.

Actively participate in data governance boards and cataloging efforts. Such participation helps build awareness and literacy about institutional data management and develop greater alignment of business processes across the institution.

Maintain compliance with the standards set by the ISO. These international standards improve privacy and security and decrease risk. Departments and units will need systems to track compliance as well as education and training so that all stakeholders know how to maintain compliance.

Multi-Institution Collaboration

Multi-institution collaboration in higher education refers to partnerships and coordinated efforts between colleges, universities, or educational organizations to achieve shared goals, enhance resources, and address common challenges. These collaborations can occur at various levels including regional, international, system-wide, and cross-consortia collaborations.

Leverage professional associations to share a collective understanding of privacy and security laws, requirements, and frameworks. Professional associations not only help institutions connect and collaborate but also provide institutions with resources to help define and interpret regulations and standards, stay abreast of news and trends, and more. Associations also bring together stakeholders from institutions and industry, creating more opportunities for collaboration.

Form system-wide committees to create policies and strategies and implement long-term solutions. Multi-institution collaboration within systems may be facilitated by existing infrastructure, making such collaboration a great starting point.

Create industry-wide agreements not to pay ransomware attackers. Disincentivizing bad actors reduces risk across higher education.

Build a unified AI governance standard for all of higher education based on shared knowledge. Working together to create a shared standard reduces the lift for less-resourced institutions and helps higher education institutions create a strong foundation for navigating quickly evolving AI technologies.

Participate in lobbying lawmakers to address higher education concerns. Such lobbying may help lawmakers understand higher education's needs as well as its value to the public. More communication with lawmakers could introduce more efficiency in higher education policy, but all stakeholders involved must be careful to not let communications slow their decision-making.

Share achievements across institutions to support motivation, momentum, and friendly competition. Sharing progress improves morale and supports problem solving. Certainly, institutions should be cautious about oversharing, which could lead to providing inside information to bad actors.

PLANNING FOR THE ROAD AHEAD

Strategic foresight is only a useful tool if it helps us move from insight to action, creating the future we want to see. Use the following activities to solidify your vision of the future and make plans to take action.

Your Role in the Future of Supporting Agency, Trust, Transparency, and Involvement

As you embark on the journey, consider the following questions:

- What role do you want to take in these plans?
- Will you start with individual action, or do you want to lead collaborative efforts?
- What is the current state of supporting agency, trust, transparency, and involvement at your institution, and where will your institution be 10 years from now?

Activity: Understand Your Institution's Needs

The best plan of action always starts with understanding the starting line. Use this activity to explore the current needs and interests of stakeholders at your institution.

- Make a list of key stakeholders at your institution who will be interested in shaping the future of supporting agency, trust, transparency, and involvement. Consider a wide range of perspectives from a variety of operational units: academic units, information technology, information security, privacy, student services, legal, etc.
- Select a sample of individuals from your list and talk to them about the present and future state of supporting agency, trust, transparency, and involvement at your institution. Some guiding questions are:
 - What is our current state of supporting agency, trust, transparency, and involvement?
 - How do we currently support agency, trust, transparency, and involvement?
 - What are our biggest challenges related to supporting agency, trust, transparency, and involvement?
 - What are our greatest assets related to supporting agency, trust, transparency, and involvement?
- Take notes on key takeaways from your conversations. Include references for resources and documents such as websites and institutional policies.
- Reflect on your findings and consider how they align with the findings in this report. Is your institutional vision aligned with our panelists' ideas? Are any individuals at your institution ready to take some of the actions described in this report?
- Make a plan for next steps. Usually, this starts with identifying key members of your professional network who can partner with you. Consider stakeholders who are ready to hit the ground running, colleagues who already have considerable influence and can break down barriers, and colleagues or units that might be resistant to change and need help seeing your vision.

Activity: Build an Action Roadmap

Now that you have a clear picture of where you are, where you want to go, and who is going to help, you're ready to develop an Action Roadmap from the [Institute for the Future](#). This activity is best accomplished collaboratively, so consider working with some of the individuals you identified in Understand Your Institution's Needs. Start with the right side of this tool, describing the goals and elements of *your* preferred future, using the future described in this report as inspiration. Then review the findings you generated with Understand Your Institution's Needs and describe the short-, mid-, and long-term actions that will carry you from today's reality to the future you want to see.

BUILD AN ACTION ROADMAP

Short-term _____

Mid-term _____

Long-term _____

Milestones

Milestones

Milestones

Easier Activities

Easier Activities

Easier Activities

Harder Activities

Harder Activities

Harder Activities

Describe your preferred future

© 2023 Institute for the Future. All rights reserved. SR-2300B | CC BY-NC-ND 4.0

More Resources for Taking Action

As you work toward supporting mental health at your institution, be sure to explore these resources:

[EDUCAUSE Cybersecurity and Privacy Program](#)

[Cybersecurity and Privacy in EDUCAUSE Review](#)

[2024 EDUCAUSE Horizon Report | Cybersecurity and Privacy Edition](#)

[EDUCAUSE Higher Education Community Vendor Assessment Toolkit](#)

[EDUCAUSE Cybersecurity Community Group](#)

[EDUCAUSE Cybersecurity and Privacy Managers Institute](#)

[EDUCAUSE Events](#)

2025 EDUCAUSE Horizon Action Plan: Supporting Agency, Trust, Transparency, and Involvement

9

This *2025 Horizon Action Plan: Supporting Agency, Trust, Transparency, and Involvement* is grounded in the perspectives and knowledge of an expert panel of practitioners and thought leaders representing the higher education cybersecurity and privacy community. The members of this group were sought out for their unique viewpoints, as well as their contributions and leadership within their domain.

For this action plan, we adopted and adapted different components of the Institute for the Future foresight methodology. First, we asked panelists to review the trends, technologies and practices, and scenarios from the *2024 EDUCAUSE Horizon Report: Cybersecurity and Privacy Edition* and to describe their own vision of the preferred future of higher education. Second, panelists were directed to list the threats and opportunities that might imperil or bring momentum to their preferred future and to brainstorm possible actions in response to those threats and opportunities. The data produced as a result of these efforts have been used to create the action plan featured in this report.

EDUCAUSE researchers provided group facilitation and technical support but minimal influence on the content of the panel's inputs and discussions. This was done to reduce the potential introduction of bias into the results and to allow for this organized group of experts themselves to discuss and converge on a set of actions for the future, based on their own expertise and knowledge.

The panel discussions were held remotely on January 16, 2024, by Zoom.

EXPERT PANEL ROSTER

We would like to acknowledge and express our deepest gratitude to the panel of experts listed below who were responsible for generating all of the big ideas summarized throughout this resource. Their brilliant thinking and rich discussions were the foundation of this work, and this resource simply would not exist had it not been for their dedication to this project and their passion for serving higher education.

Ben Archer

Privacy Manager
Arizona State University

Jill Rasmussen

Identity and Access Management, IT Security
University of Rhode Island

Joe Gridley

Chief Data Privacy Officer
University of Maryland

Lydia Payne-Johnson

Director, Data Governance, Compliance, and
Identity Management
The George Washington University

Mike Hanson

Information Security Engineer
Ithaca College

Venkata (Sirish) Malisetty

California State University, Northridge
Data and Analytics Lead

Wendy Epley

Principal Analyst, Information Security–
Governance, Risk, and Compliance
University of Arizona

Isaac J. Galvan

Director, Cybersecurity and Privacy Program
EDUCAUSE

Jenay Robert

Senior Researcher
EDUCAUSE

Nichole Arbino

Senior Program Manager
EDUCAUSE

Keturah Young

Communities Program Manager
EDUCAUSE