

**From:** [McMorries, David W](#)  
**To:** [Inform-C06 \(Classified\)](#); [Inform-C07 \(Professional Faculty\)](#); [Inform-C08 \(Instructors, Research Associates/Assistants\)](#); [Inform-C09 \(Professors, Associate/Assistant Professors\)](#); [Inform-c12 \(Academic Wage & Other Misc\)](#); [Inform-C14 \(Graduate Assistants\)](#)  
**Subject:** Safeguarding OSU: Guidance on Third Party Information Security Risks  
**Date:** Thursday, January 22, 2026 10:30:38 AM

---

Dear OSU Community,

Oregon State University partners with external vendors to enable innovation and operational efficiency across a wide range of applications, including AI tools, cloud storage and procurement systems. OSU has streamlined procurement processes by using BennyBuy and Travel and Expense-card credit transactions to obtain goods and services. While these partnerships and processes offer significant benefits, they also introduce potential risks that require awareness and diligence to protect the OSU community and university assets.

Third-party vendors may store confidential and sensitive data on behalf of OSU. The type of data a vendor holds directly impacts the risk involved. Vendors storing confidential or sensitive university data pose a higher risk than those storing publicly available information. A breach or service disruption involving a key vendor could impact university operations, research, and extension services.

Common technologies available through third-party vendors may not provide adequate security protections for OSU data. To address this, the Office of Information Security (OIS) partners with the Office of Procurement, Payment, and Travel (OPPT) and the Office of General Counsel (OGC) to evaluate all third-party IT procurements. These evaluations follow established best practices to ensure clear contractual responsibilities and assess security risks in alignment with institutional standards.

-  
Guidance is being developed to help the OSU community understand risks, including those associated with AI and other emerging technologies. The following resources are available to support you when engaging with third-party vendors:

- [Third-Party Vendor Information Security Risk Management Rule](#) (Accessible with an ONID)
- [Procurement, Payment and Travel](#)

If you become aware of a potential third-party risk or incident, report it immediately to OIS.

By working together, we can ensure that OSU's community, data and operations remain secure, resilient, and compliant.

Respectfully,  
Hanna and David

Assistant Vice President and Chief Procurement Officer Hanna Emerson

Assistant Vice Provost and Chief Information Security Officer David McMorries

**David McMorries**

Chief Information Security Officer, Office of Information Security

**Oregon State University** | University Information and Technology | 541-737-9561