



**The 2026 Dewald Roode Workshop on Information  
Systems Security Research (IFIP WG8.11/11.13)**  
October 9-10, 2026  
The University of Arizona, Tucson, Arizona

## Call for Papers

The 18th Dewald Roode Workshop on Information Systems Security Research will continue the efforts to advance the discipline of information systems security through the creation, dissemination, and preservation of well-formed research, following the success of the first seventeen workshops (University of Cape Town, 2009; Bentley University, 2010; Virginia Tech, 2011; Brigham Young University, 2012; University at Buffalo, 2013; Newcastle University, 2014; University of Delaware, 2015; University of New Mexico, 2016; University of South Florida, 2017; University of Cape Town, 2018; Louisiana Tech University, 2019; Iowa State University, 2020; University of Texas at San Antonio, 2021; University of Colorado Denver, 2022; University of Strathclyde, 2023; Kennesaw State University, 2024; United States International University-Africa, 2025).

The active discussions in the workshop are intended to provide participants with specific and actionable feedback on their research. We anticipate that this process will facilitate the development of workshop papers for further consideration in important journals. Selection for the workshop is competitive, and only authors of the accepted papers and active working group members will be invited to participate. High-quality accepted papers may have the opportunity to be fast-tracked in a special issue at *Information Systems Frontiers* (please see here for more details <https://link.springer.com/collections/egdbefhiee>).

Anchoring the workshop to information systems means that the research will attend to and extend the social, organizational, and managerial literature in the focal area. We welcome a wide range of methodological lenses, including behavioral, design-science, econometric, qualitative, and computational (e.g., optimization and simulation) approaches, provided they advance our understanding of the human and organizational side of security. While we assume an effective foundation in information security technology, we regard information systems risk broadly, for example, computer crime, employee misconduct, cyber warfare, cyber terrorism, human error and/or accident, natural events, etc. We also address information systems security broadly, for example, policies and policy compliance, diverse security behaviors, privacy, awareness, strategy, audit, planning, and control. These and related research topics will be the focus of this workshop.

### TOPICS OF INTEREST:

The 2026 Dewald Roode Workshop on Information Systems Security Research Topics may include (but are not limited to):

- Theoretical and empirical analyses of information security behavior
- Adoption, use, and continuance of information security technologies and policies
- Compliance with information security and privacy policies, procedures, and regulations
- Investigations of computer crime and security violations
- Motivators and inhibitors of employee computer crimes
- Forensic analysis of security breaches and computer crimes
- Individual, organizational, and group information privacy concerns and behaviors
- Legal, societal, and ethical issues in information security

- Neurosecurity (NeuroIS) investigations of information security behavior
- Behavioral analyses of design science treatments enhancing or balancing security and privacy tradeoffs
- The behavioral intersection of cybersecurity/privacy research and AI/ML advancements

### SUBMISSION INFORMATION:

- **Format:** The paper length requirement is 15-25 pages double-spaced for double-blind review.
- **Submission deadline:** **June 27, 2026.**
- **Notification to authors:** **August 1, 2026.**
- **Deadline for final papers:** **August 17, 2026** (to be distributed to workshop attendees in advance)
- **Registration:** Attending participants must register by **August 15, 2026.**
- **Late registration:** **September 1, 2026**
- **Paper submission link:** <https://cmt3.research.microsoft.com/DRW2026>

### CONFERENCE LOGISTICS:

#### General Chair:

- Matthew Hashim, The University of Arizona, [mhashim@arizona.edu](mailto:mhashim@arizona.edu)

#### Program Co-Chairs:

- AJ Burns, Louisiana State University, [ajburns@lsu.edu](mailto:ajburns@lsu.edu)
- Yuan Li, University of Tennessee at Knoxville, [yli213@utk.edu](mailto:yli213@utk.edu)
- Laura Amo, University at Buffalo, [lccasey@buffalo.edu](mailto:lccasey@buffalo.edu)

The program co-chairs will prescreen manuscripts to ensure that manuscript submissions are reasonably complete, well-formed, and appropriate to the scope and mission of the workshop. Double-blind reviews will follow for prescreened papers. Authors can submit the manuscripts as “early stage” or “completed papers.” Manuscripts must be anonymous for the review process.

In recognition that the review process greatly relies upon a scarce resource of the services of reviewers, authors, by the act of submission, are implicitly promising to serve as a reviewer on one to two conference papers, if requested.

For general questions about the workshop, please contact Matthew Hashim. For questions about the program, please contact Laura Amo.

### WORKSHOP DATE AND LOCATION:

The workshop will be hosted by The University of Arizona and will take place on October 9-10, 2026. There are several hotels and restaurants located within walking distance from the University, with a hotel block available from October 8-10 at the Graduate Hotel using the following link: <https://book.passkey.com/e/51272252>. Please continue to view the following website for more details on this year’s conference as they become available: <https://eller.arizona.edu/events/dewald-roode-workshop-information-systems-security-research>

### SPONSORSHIP:

The IFIP Working Group 8.11/11.13 holds The Dewald Roode Workshop on Information Systems Security Research annually. WG 8.11/11.13 (Rui Chen, Chair; Phil Menard, Vice-Chair) is the IFIP Working Group on Information Systems Security Research.

Please visit <https://sites.google.com/view/ifip-working-group> for more information on the IFIP Working Group 8.11/11.13 and past workshop proceedings.