Dear UTA community,

The University of Texas at Arlington continues to work with law enforcement and external experts to investigate and address a cybersecurity incident first discovered on Oct. 26, 2026.

The investigation now indicates that personal information was accessed during the incident. We are working to determine whose information may have been involved and the nature and extent of the information accessed. Once we have identified the individuals affected, we will contact them directly with information about what happened, steps they can take to help protect their information, and how the University will support them. We are committed to keeping those affected both informed and supported through this process.

We are also taking additional steps to strengthen our cybersecurity protections and safeguard the information entrusted to us. This includes enhancing security measures and reviewing our systems and processes to reduce the risk of similar incidents in the future.

Please refer to our official cybersecurity incident webpage for official updates and answers to frequently asked questions.

Operational impacts

As a result of the incident, MachForms remain offline. We recognize that this interruption is affecting important work across the University. Anyone with an urgent and significant operational need for an alternative to MachForms should contact the Office of Information Technology (OIT) Service Desk at https://www.uta.edu/help/.

How you can help

Protecting university information and maintaining essential operations remain top priorities. We will continue to share timely, accurate updates as appropriate. We continue to ask all employees and students to help with the following:

- **Follow official guidance**. Pay attention to University communications and follow instructions from OIT and the Information Security Office. Official updates will be posted to www.uta.edu/cybersecurity.
- **Report suspicious activity**. If you notice unusual computer behavior, receive a suspicious email or encounter anything else that raises cybersecurity concerns, report it to opsec@uta.edu. Do not click unfamiliar links or open unexpected attachments.
- **Rely on verified information**. Direct questions to your department head or OIT and rely on official updates for confirmed information. If you are contacted by a journalist, please direct them to UTA's media relations team.
- **Follow any additional instructions**. If action is needed involving passwords, devices, systems or work practices, employees and students will receive specific guidance through official University channels.

We understand the uncertainty this incident is causing across UTA and the broader higher education community. We appreciate your patience, understanding and cooperation as we work to resolve these challenges.

Sincerely,
Archie L. Holmes Jr.
Acting President