



University of Idaho
Office of Information Technology

OIT Newsletter for Instructors

Fall 2022

Zoom Cloud Recordings Automatically Moved to OneDrive

Cass Hall

All new Zoom cloud recordings are now sent to a OneDrive folder and deleted from the Zoom cloud. This change was made to keep all U of I Zoom recordings secure and comply with FERPA regulations.

You will receive an email titled "Zoom to OneDrive Upload" after a recording has been processed. To access the recording, click on the link provided in the email. There is a link directly to the recording and a link to your Zoom-Recordings folder.

Recordings in OneDrive can be shared with individuals or Canvas groups or embedded into Canvas.

- [Get more details on accessing and sharing your Zoom videos in OneDrive](#)
- [Learn how to embed a video from OneDrive into Canvas](#)
- [View FAQs](#)

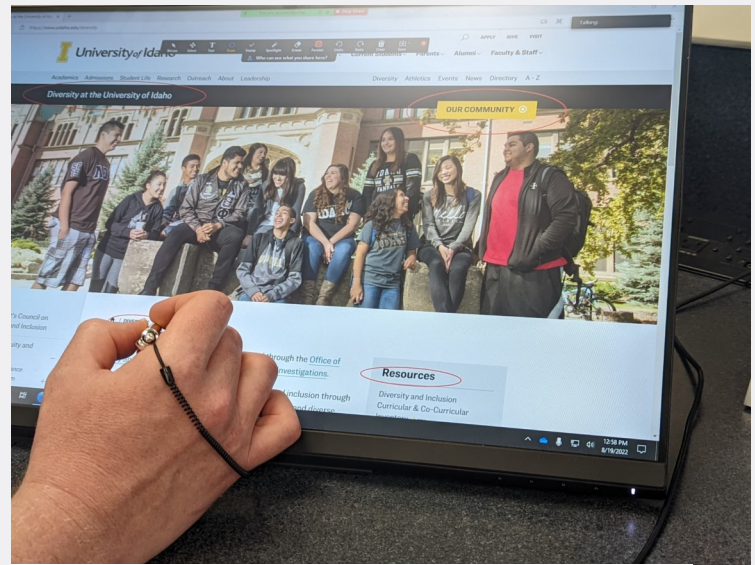
Email questions to ccts@uidaho.edu. Register for a Q&A session on page 3.

The screenshot shows an email notification from the University of Idaho. The header includes the University of Idaho logo and navigation links for "Your Account" and "Request Assistance". The main body of the email states: "Your recent Zoom meeting recording files have been successfully uploaded to your OneDrive 'ZoomRecordings' Folder. These recordings are not available in Zoom." Below this, there are two blue hyperlinks: "Information on how to embed your OneDrive recordings in Canvas" and "Information on how to access and use your OneDrive ZoomRecordings folder". A list of meeting details follows: Meeting ID (blurred), Meeting Host (blurred), Meeting Topic: "Recording Test", Meeting Start Time: "08/17/2022 09:20:29", OneDrive Video Link: "2022-08-17.09-20-47 - Recording Test.86830941679.MP4", and OneDrive Folder Url: "ZoomRecordings".

Stepping Up Instructional Support for Classroom Technology

Cass Hall

Collaboration and Classroom Technology Services (CCTS), which is part of the Office of Information Technology (OIT), is focused on improving the information that instructors receive about General University Classrooms (GUCs). Help articles have been created on each room type with a culminating article that lists all classrooms by type and provides links to all support articles. This information was also sent to instructors in an email before the beginning of the semester. If you did not receive or would like us to resend it, please contact ccts@uidaho.edu.



Instructor using a touch monitor in an enhanced video conferencing classroom

See the following article for a list of technologies in all GUCs and instructions for using each type of system: [What technology is in classroom spaces on the Moscow campus?](#)

[Multimedia Instructions \(link\)](#)

AD 317 & 336
AG SCI 204
ALB 202 & 335
BEL 205
BPC 040A
CNR 010
EP 122, 214, 216
JEB 221 & 328
LSS 163
MCCL 415
NICCOL 006 & 301
REN 127
TLC 022, 028, 031, 032, 040, 041, 044, 045, 050, 051, 122, 139, 140, 141, 144, 145, 146, 147, 149, 222, 223, 241, 244, 245, 246, 247, 249

Multimedia lecture halls with mic improvements

See [multimedia link](#) for basic instructions

See [mic instructions \(link\)](#)

AG SCI 106
JEB 104
LSS 277
REN 111 & 112

Multimedia with dual projectors/displays

See [multimedia link](#) for basic instructions

See [dual projector/display instructions \(link\)](#)

ALB 101, 012, 201, 204
ED 141
REN 125 & 126
ED 243, 442, 443

[Zoom Enabled \(link\)](#)

AAS 103
AD 301 & 307
BEL 116, 118, 346
CNR 209
LLC 132, 133, 144
MCCL 115 & 117
MINES 212, 214, 306
NICCOL 206
REN 129 & 132
SHOUP 307

[Video Conferencing Instructions \(link\)](#)

EP 202 & 204
NICCOL 208

[Enhanced Video Conferencing Instructions \(link\)](#)

AD 277 & 326
ALB 112 & 212
EP 205 & 209
MCCL 209 & 315
TLC 023, 030, 046, 047, 148

[Enhanced Video Conferencing with Video Tracking Instructions \(link\)](#)

TLC 029 & 248

[BYOD - Bring Your Own Device Instructions \(link\)](#)

MINES 217 & 219

[TEAL - Technology Enhanced Active Learning Instructions \(link\)](#)

ED 441

Register for Upcoming Workshops

Teaching in UI's High-Tech Classrooms to Enhance Hybrid Learning

Audrey Fu

1:30 p.m., Tuesday, August 30, 2022

TLC 029 or via [Zoom \(link\)](#)

This workshop will demonstrate how to enhance hybrid learning when teaching from the Moscow campus classrooms TLC029 & TLC248. Parts of this workshop also apply to the following classrooms: AD227, AD326, ALB112, ALB212, EP205, EP209, MCCL209, MCCL315, TLC023, TLC030, TLC046, TLC047, and TLC148.

Topics Covered:

1. How to set up and adjust the auto tracking camera
2. How to use the touchscreen monitor
3. How to use the doc cam inside Zoom
4. How to involve students online
5. How to record the lecture to the Zoom cloud and then access, download, and share the recording.

[Register Now!](#)

Zoom Cloud Recordings to OneDrive Q & A

Collaboration & Classroom Technology Services (CCTS)

9:30 a.m., Tuesday, September 6, 2022 via [Zoom \(link\)](#)

[Register Now!](#)

All new Zoom cloud recordings are now automatically sent to OneDrive and deleted from Zoom. Each time you record to the Zoom cloud, you'll receive an email once the recording is ready in OneDrive.

Join us if you have any questions about this process. We'll also cover: how to access the recordings in OneDrive, how to share the recordings, and how to embed the recordings in Canvas.

Zoom Whiteboards & Other New Features

Collaboration & Classroom Technology Services (CCTS)

9:30 a.m., Tuesday, September 20, 2022, via [Zoom \(link\)](#)

Zoom Whiteboards have many new features, including: building whiteboards before a meeting, collaborating in whiteboards during or outside of a meeting, adding up to 12 pages within one whiteboard. This workshop will demonstrate the use of whiteboards, then we'll dive into new features within Zoom Breakout Rooms and other things new to Zoom.

[Register Now!](#)

University of Idaho

REMOTE COMPUTER ACCESS

VLAB has been Replaced by the Remote Access Lab

Darren Kearney

Over the summer the VLAB service was discontinued in order to provide a better experience for users through the Remote Access Lab (RAL) which provides the same software. RAL is available for all students to access using the new URL <https://www.uidaho.edu/remotelab>. A VPN connection is required to connect to the service. More information on connecting to the RAL can be found at the knowledgebase article "[Remote Access Lab Connection Guide](#)".

University Dashboard Released as Beta

Jason Swanby

A new university dashboard called [MyUI](#) is available to all students this fall as a beta version. MyUI offers a personalized dashboard with access to content and real-time data via configurable "cards". Full functionality will be available by the 2023-24 academic year, ultimately providing a one-stop shop for students' digital university needs. More info is available at www.uidaho.edu/its/myui.



Major Updates to Information Technology University Policies

Teresa Amos

Three university policies concerning information technology have had major updates. Please take time to review and understand the policies. [APM 30.16](#) Technology Life Cycle includes new purchasing requirements. [APM 30.12](#) Acceptable Use was updated to include protocols that hide the location and identity of the user. This update will require you to accept the new Terms of Use when authenticating in the near future. [APM 90.35](#) U of I Credential (Vandal Card) has been updated and streamlined.

[APM 30.16](#) Technology Hardware Lifecycle Management requires technology hardware as defined in the policy be purchased through OIT regardless of funding source. Standard technology hardware will be purchased unless the standard does not meet the requirements or specifications of intended use for the hardware; exceptions must be preapproved. Noncompliance may include technology hardware disabled or removed from university network; blocked from accessing University systems; and/or technology hardware returned to the vendor.



University of Idaho
Office of Information Technology

Back to School Cyber Safety

Mitch Parks

Being safe with your accounts, your research, and university data, has never been more critical. Attackers routinely target U of I accounts to get access to intellectual property, including both university research and our journal access, to use our accounts to target others inside and outside the university, to trick people to fall for gift card or job scams, or even change your direct deposit!

Following the tips below will reduce the risk that you will become a victim of cybercrime.

Watch out for social engineering in email and other messaging

- Refrain from clicking links in unexpected emails or text messages.
- Don't download or open attachments you were not expecting
- Only enter your U of I credentials at uidaho.edu or microsoftonline.com
- Only use your U of I email for official communications, and not any free-mail accounts
- Take a pause - don't open an email when it first arrives - malicious messages are sometimes cleaned up after delivery
- Report suspicious emails with the "Report Phish" button in the upper right of your email toolbar



Protect university systems and our data

- Install security updates as they become available, typically at least once a month
- Close your web browser routinely - at least once a week, so it can auto-update
- Use your university-managed devices and accounts for handling U of I data
- Always use encryption where required - contact your TSP if you need to encrypt your computer
- Only share data with those who have a legitimate U of I need and interest
- Store data only in [approved storage locations \(link\)](#)

Practice good password hygiene

- Use strong, unique passwords for every account and enroll in multi-factor authentication where possible
- **Never approve unexpected Duo notifications**
- Never use your U of I password on any other account
- Ensure the answers to your security questions are not publicly available
- Consider using a password manager to store and remember passwords

Report suspicious events with your computer or accounts to your TSP or security@uidaho.edu

It takes all of us to ensure the University of Idaho is protected from cyber criminals. Take time to set yourself up for success, and Go Vandals!