MONTANATECH WEEKLY UPDATE

December 18, 2023

IN THIS EDITION

2024 MBMG Calendars

Turnit In Training Session

Security

UPCOMING CAMPUS EVENTS

12/19: Pilates (12:00 pm, HPER)

12/21: Weights (12:00 pm, HPER)

12/25: Christmas Day

12/28: WBB vs Lakeland College (2:00 pm, HPER)
MBB vs Lakeland College (4:00 pm, HPER)

12/29: WBB vs Ambrose University (2:00 pm, HPER)
MBB vs Ambrose University (4:00 pm, HPER)

01/01: New Year's Day

01/11: Turnitin Training (3:30-5:00 pm, Eng Hall 106)

2024 MBMG CALENDARS ARE HERE

The Montana Bureau of Mines and Geology's 2024 calendars are available for distribution from the Bureau Publication Office in the Natural Resources Building. Each campus employee can pick up a complimentary calendar; we ask that you sign for it so we can keep track of distribution. If a department or other group wants to have one person collect for everyone, just bring a list of names to be checked off. Additional copies can be purchased for $5.00 each. Montana Geologic Map Jigsaw Puzzle – 1000 pieces (20 x 28 inches) or 504 pieces (16 x 20 inches) for $30.00 each available through our publications office.

TURNIT IN TRAINING SESSION

Montana Technological University subscribes to Turnitin, text-matching identification software that can help instructors detect the presence of plagiarism,

contract cheating, and AI-generated text in students' papers. This powerful tool also simplifies remote assignment submission and has built-in electronic grading functions that significantly speed up the marking process. The next Turnitin training session is scheduled for **Thursday, January 11 from 3:30 until 5:00** in Engineering Hall room 106. Please consider attending this session if you are curious about Turnitin's AI detection and grading tools, have never used Turnitin, or want a Turnitin refresher.

SECURITY

Phishing, Malware, and Ransomware are all terms we covered during October as a part of cyber security awareness. Did you know storing your password in your web browser (Firefox, Chrome, Edge) is just as dangerous? Attackers are now trying to trick users into clicking links (often in an email) that will install software to steal those passwords saved in a web browser. The best practice is to use a different password for each site and store it in a password manager such as KeePass, BitWarden, etc. We highly recommend enabling multifactor authentication for all your accounts where available.