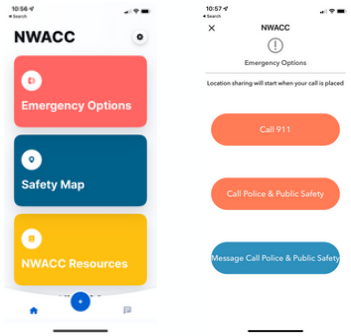
# POLICY, RISK MANAGEMENT & COMPLIANCE

*October 2023 Issue*

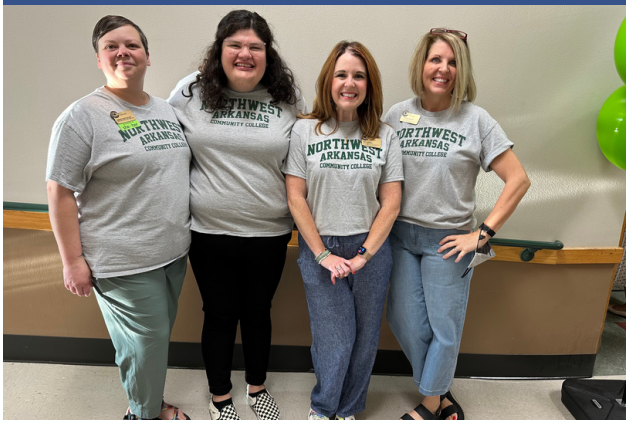
*prc@nwacc.edu*

## HAVE YOU DOWNLOADED LIVESAFE YET?




## MEET THE STAFF

**Kim Bertschy**
Director of Policy and Compliance
**Darcy Castaneda**
Administrative Analyst
**Erin Campbell**
Director of Risk Management
**Teresa Taylor**
Executive Director of Institutional Policy, Risk and Compliance / Title IX Coordinator



## WHAT IS FOIA?

"The Arkansas Freedom of Information Act (FOIA) allows the public to inspect & receive copies of public records of governmental agencies unless the law makes an exception for them. The law also requires that most meetings of "governing bodies" be open to the public.The Arkansas Freedom of Information Act (FOIA) allows the public ("citizens") to inspect and receive copies of public records of governmental agencies unless the law makes an exception for them. The law also requires that most meetings of "governing bodies" be open to the public."

If you receive a FOIA request, please notify **Erin Campbell (ecampbell7@nwacc.edu)** immediately. You can find more information on Arkansas FOIA here: https://www.nwacc.edu/administrativeservices/riskmanagement/emergencyresponsebusinesscontinuity/arkansasfoia.aspx

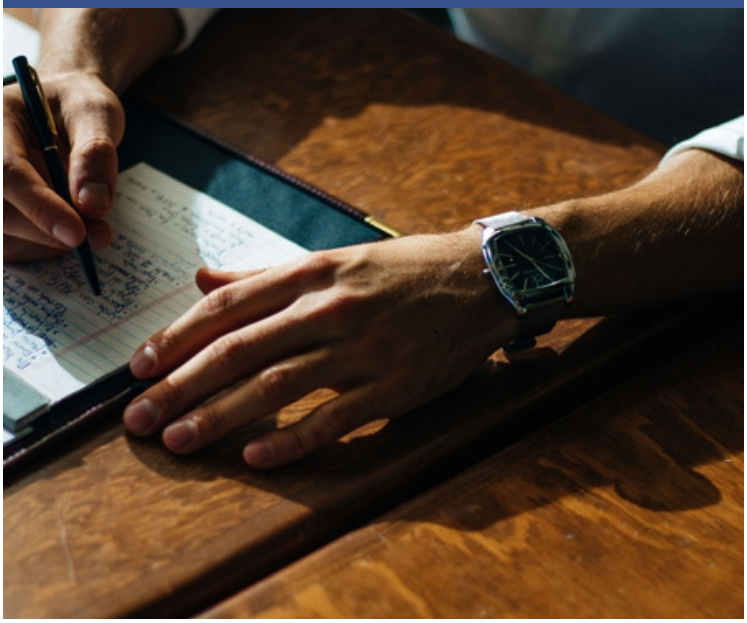
# POLICY, RISK MANAGEMENT & COMPLIANCE

*October 2023 Issue*

*prc@nwacc.edu*

## CLERY CORNER

The safety and security of our campus is a collaboration by staff, faculty, administration, students, parents and community groups. Annually, the College publishes a Security Report that includes campus crime prevention information, security policies and crime statistics. Disclosure and accurate reporting of this information is required by law. It is important for all members of the campus community to be familiar with how to report incidents and participate in safety training sessions offered virtually or in person.



PRIDE at NWACC

The Title IX Office is partnering with Pride at NWACC to offer Safe Zone training for those interested in learning more about LGBTQ+ issues and allyship. Safe Zone Training is a program aimed at reducing homophobia, transphobia and cisheterosexism at NWACC and in our surrounding community, thereby making a safer environment for all members of our community across sexual orientations, romantic orientations, gender identities, gender expressions and intersections of identities. Faculty, staff and student session will be offered. Registration is required.

Use the QR code to access the registration link with session dates.

Departments or student groups interested in a Safe Zone session or other workshops may contact pride@nwacc.edu

## VECTOR COMPLIANCE TRAINING

Did you know our Vector LMS has a library of on demand training? There are several modules available for employees that can be completed at any time. The Student LMS launch is underway. The student platform features prevention programs, safety, and wellness courses. We can also create custom courses in both our employee and student sites. If your department has a specific need for employee or student training please contact PRC at prc@nwacc.edu!

Vector Solutions

# POLICY, RISK MANAGEMENT & COMPLIANCE

*October 2023 Issue* *prc@nwacc.edu*

## OCTOBER IS CYBERSECURITY AWARENESS MONTH!

**This month and year round PRC encourages everyone to help make our digital presence safer. Here are four simple steps that can help you stay safe online.**

### USE STRONG PASSWORDS

**Using an easy-to-guess password is like locking the door but leaving the key in the lock. Weak passwords can quickly be cracked by computer hackers. The good news is that strong passwords are one of the easiest ways to protect your accounts from compromise and reduce the risk of someone stealing sensitive information, data, money, or even your identity.**

**FOLLOW THESE TIPS:**

**1. Longer is stronger: Passwords with at least 16 characters are hardest to crack.**

**2. Hard to guess: Use a random string of mixed-case letters, numbers and symbols. If you need to memorize a password, create a memorable "passphrase" of 5 – 7 unrelated words. Get creative with spelling and/or add numbers or symbols**

**3. One of a kind: Use a unique password for each account.**

### UPDATE SOFTWARE

**Keeping software up to date is an easy way improve your digital security. For added convenience, enable automatic updates on software so the latest security patches keep devices continuously updated.**

**FOLLOW THESE TIPS:**

**1. Check for notifications Devices and applications will usually notify you when the latest software updates become available, but it's important to check periodically as well. Software updates include devices' operating systems, programs and apps. It's important to install ALL updates, especially for web browsers and antivirus software, or apps with financial or sensitive information.**

**2. Install updates as soon as possible When a software update becomes available, especially critical updates, be sure to install them as soon as possible. Attackers won't wait, and you shouldn't either!**

**3. Turn on automatic updates With automatic updates, devices will install updates as soon as they become available —Easy! To turn on the automatic updates feature, look in the device settings, usually under Software or Security**

Be an Eagle Eye, Verify

**PAUSE** Before clicking links or opening attachments in email

**VERIFY** the URL or sender

**REPORT** suspicious content to techsupport@nwacc.edu


### TURN ON MULTIFACTOR AUTHENTICATION

**Multifactor Authentication (MFA) provides extra security by providing a secondary method confirming your identity when logging into accounts. MFA usually requires you to enter a code sent to your phone or email, or one generated by an authenticator app. Push notifications are also common methods of MFA. This added step prevents unauthorized users from gaining access to your accounts, even if your password has been compromised.**

### Be an Eagle Eye, Verify

Recognize and report phishing. Phishing attacks have become an increasingly common problem for organizations of all sizes and can be very difficult to spot. It's important every individual stop and think before clicking on a link or opening an attachment and know how to spot red flags. Phishing occurs when criminals try to get you to open harmful links or attachments that could steal personal information or infect devices. Phishing messages or "bait" usually come in the form of an email, text, direct message on social media or phone call. These messages are often designed to look like they come from a trusted person or organization, to get you to respond. The good news is you can avoid the phish hook and keep accounts secure!

### FOLLOW THESE TIPS:

1. Recognize - Look for these common signs: Urgent or alarming language, requests to send personal and financial information, poor writing, misspellings, or unusual language, incorrect email addresses, domain names, or links (e.g. amazan.com)
2. Report - If you suspect phishing, report the phish to protect yourself and others. Report phishing to IT. For personal email accounts, you may be able to report spam or phishing to your email provider by right-clicking on the message
3. Delete - Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. Just delete.