

Managed Ongoing Awareness & Trust

Award-winning Security Awareness/Policy Management/Risk Management Tools



The **Managed Ongoing Awareness & Trust (MOAT)** web-based platform from Awareity provides organization's with all the right tools to manage training and policies, on an ongoing basis and review compliance reports in real-time.

Benefits:

- Award-winning Information Security Awareness training modules
- Confidential Awareness Vault for uploading customized, organization and role specific training
- Real-time reporting and documentation for tracking annual certifications and training for audits and accreditations
- Meet compliance obligations and requirements across the organization
- Track employee and third-party acknowledgements required by state and federal mandates
- Customized Incident Reporting for Users to report suspicious activities and red flags
- Incident Management tracking and documentation of actions taken to intervene and prevent incidents (Workplace Violence, Harassment, Bullying, Weapons, Drug/Alcohol Abuse, Ethics, Fraud, Threat to Harm, OSHA, Clery Act, Information Privacy, Safety, Emergencies, etc.)

MOAT Security Awareness Training:

Awareity's Security Awareness Training (SAT) ensures your people are aware of information security requirements as defined by SEC-501, as well as ISO-27001, HIPAA, FERPA, PCI-DSS, FACTA Red Flag Rule and others. The SAT modules are updated annually or as needed with the most up-to-date information regarding security risks, threats, best practices, lessons learned and regulatory updates so your organization can focus on specific needs. Case studies and news stories are strategically placed in the modules to help Users connect real-world events to your organizational policies and requirements. Each module consists of multiple lessons and includes one or more questions to ensure all Users understand key topics, risks and threats. Each question must be answered correctly to achieve their certification.

Lessons include:



- **Information Risks** (Electronic and non-electronic information risks, identity theft, physical security, etc.)
- **Internet Security** (Internet security, Internet risks, Internet best practices, online security, mobile information security, etc.)
- **E-mail Security** (E-mail awareness, e-mail risks, phishing and pharming, e-mail usage, etc.)
- **Human Factor Risks** (Human factors, password security, social engineering, incident management, etc.)

All Users receive an initial notification requiring them to login and complete the Security Awareness Training Modules. All User activity is tracked and documented and automatic reminders are generated by MOAT to ensure Users (and their Supervisors if enabled) complete their certification requirements. MOAT Administrators can access on-demand User Progress reports to monitor User activity, including login times, responses, document acknowledgements, and all reports are printable and downloadable.

All Users automatically receive certification reminders and past due notifications via e-mail until they have completed their certification requirements. No more expensive spreadsheets or labor-intensive paper-based tracking. Organizations can allow administrators or supervisors to be copied on the User messages to ensure completion and ongoing due diligence.

Each year on their individual "certification due date," the Users' SAT Modules will be automatically updated, document acknowledgements will be automatically reset, and automatic notifications will be sent so Users know to complete their annual training and policy acknowledgements.

"MOAT allows me to meet the SEC 501 standards and focus on the rest of the security demands for the college. This has helped us greatly!"

– CIO, Virginia CC

"ITD believes that MOAT Training adds value as it makes County employees aware of ongoing dangers/pitfalls and provides helpful suggestions as to how the average user can enhance security by putting these suggestions into practice. Further, the MOAT training enhances the County's efforts to keep its employees aware of their responsibilities relative to over all IT security, HIPAA compliance, and annual training compliance mandated by the Commonwealth (VITA). Educated employees are a good first step in helping to avoid unnecessary expenditures that will result when there is an IT security breach or malicious conduct."

– IT Director, Virginia County

"Security awareness training is a key component in Loudoun County Government's overall security framework. Awareity's MOAT provides our IT department with a mechanism to raise staff awareness, resulting in a better educated user community. The MOAT system is simple, flexible, and user friendly."

– IT Director, Virginia County

Helping Entities Address:

- ▣ SEC-501
- ▣ HIPAA
- ▣ OSHA
- ▣ CALEA
- ▣ ARMICs
- ▣ ISO 27001
- ▣ FERPA
- ▣ PCI-DSS
- ▣ Clery Act
- ▣ FACTA
- ▣ Emergency Preparedness (EO 41)
- ▣ Violence Prevention (EO 44)
- ▣ Environmental (EO 19)
- ▣ Threat Assessment (23-9.2:10)

MOAT: Security Awareness Training

Award-winning Security Awareness Training



Modules and Lessons:

Information Risks

- ✓ Information Risks
- ✓ Identity Theft
- ✓ Non-Electronic Information
- ✓ Physical Security

Internet Security

- ✓ Internet Security
- ✓ Internet Risks
- ✓ Internet Best Practices
- ✓ Online Security
- ✓ Mobile Information Security

E-mail Security

- ✓ E-mail Awareness
- ✓ E-mail Risks
- ✓ Phishing and Pharming
- ✓ E-mail Usage and Best Practices

Human Factor Risks

- ✓ Human Factors
- ✓ Human Factor Risks
- ✓ Password Security
- ✓ Incident Management

Social Media/Networking

Social networking sites like Facebook, LinkedIn, Twitter, YouTube and others are built on the idea of traditional social groups where you are connected to new people through people you already know. Social networking sites can also be a virtual place where users establish friendships, romantic relationships or business connections.

Social networking sites can also present security and/or privacy risks to personal and organizational information because users may perceive a false sense of security due to the lack of physical interaction. **Users also tend to submit too much information about themselves** thinking only their friends will read it, forgetting about strangers and friends of friends that may also have access to their postings. Users sometimes offer too much personal information trying to impress potential friends and associates, not realizing cyber thieves may be monitoring social networking sites and able to use this information to social engineer their way into personal assets.

Information on social networking sites that can potentially be exploited may include:

- Names
- Sexual Orientations
- Family Information (maiden name, etc.)
- Birth Dates
- Relationship Status
- Personal Interests
- Political Views
- Religious Views
- E-mail Addresses
- Schools
- Employment Information
- Photos of other friends
- Photos/Videos
- Travel Plans and Itineraries

DID YOU KNOW?
85% of people with public social media profiles shared their birthday, 63% shared their high school name, 18% shared their phone number and 12% shared their pet's name - all personal information that can be used by cyber criminals to verify your identity.

You should always review your organization's Social Media Usage policy to understand what web sites may or may not be accessed and what types of information can or cannot be shared, etc.

Best Practices for Mobile Devices

The top ten smart phone risks include: 1) Data leakage; 2) Unintentional disclosure of data; 3) Attacks on decommissioned phones; 4) Phishing (fake apps, smishing); 5) Spyware; 6) Network spoofing attacks (connecting to unauthorized wi-fi); 7) Surveillance attacks; 8) Dumpster Attacks; 9) Financial malware; 10) Network congestion (resource and network unavailability).

Although there are ways to physically protect your mobile device(s), there is no guarantee the device(s) won't be stolen or accidentally lost. Below are some best practices to follow when traveling with a mobile device:

- Keep device with you or tethered to you at all times
- In a public area, consider non-traditional bags for carrying your laptop/mobile device, so it is not an obvious target
- Set up a strong password required to access your mobile device(s)
- Install the latest updates of the operating system
- Consider storing sensitive or confidential data externally on CDs, removable disks or removable flash drives
- Encrypt sensitive data on your mobile device
- Install and update anti-virus and anti-spyware software
- Consider mobile device locator software (anti-theft software)
- Back up mobile devices often
- Connect to only secure Wi-Fi connections
- Be cautious when you are browsing web sites, opening e-mails and downloading apps

If you are using a smart phone to access work-related information, be sure you have read and understand your organization's remote access and mobile usage policies for protecting organizational data. **A recent study revealed over 40% of business users have used unsecured services to share or sync files on their mobile device, despite 87% saying they are aware their company has a document sharing policy that prohibits this practice.** 27% of these users who failed to comply with policy, reported immediate consequences! From lost business to expensive lawsuits and financial penalties of over \$2 billion, you don't want to be that employee! Next time you are thinking about sharing information or connecting your device to an unapproved location, think about taking that cut from your paycheck.

Basic Precautions Skipped
While nearly half of all smart phone users care enough about their device to sleep with them, these users are not successfully protecting them. Forty eight percent of users do not take even the most basic of precautions like using passwords, installing security software or backing up files.

What Does a Phishing Attack Look Like?

Below are some potential phrases that may indicate a phishing attack is targeting you or your organization.

"Please verify your account information."
Phishing attacks may suggest your account will be closed or suggest a system problem occurred and you need to validate your account and login information. Most organizations should never ask you to send passwords, Social Security numbers or other personally identifiable information via email, so this type of request should raise a red flag. If you receive a message asking for personal information, you should contact the organization directly to verify if the email is valid and if it is not valid you will be able to report the phishing attack so the organization can take appropriate actions to prevent others from being phished.

"You have won the lottery."
The lottery scam is a common phishing attack, also known as advanced fee fraud. These scams claim you have won a large sum of money, or that someone is going to pay you a large sum of money for little or no work. The lottery scam will most often include a reference to a well-known company, such as Microsoft, but there is no Microsoft lottery.

"If you don't respond within 48 hours, your account will be closed."
Some phishing messages convey a sense of urgency so that you'll respond immediately without thinking or questioning if the request is valid. Verify suspicious e-mails by making a direct phone call to the company from which the e-mail appears to originate and ask, if the e-mail is legitimate. If you prefer to verify the suspicious e-mail by contacting the company's web site, you should type the web site address into your web browser address bar rather than clicking the link provided in the e-mail message. By taking these verification steps, you can protect your organization and yourself from expensive incidents and embarrassing headlines.

Data Encryption for Data in Transit

Encryption is a good way to protect sensitive information while the information is being transmitted or while the data is stored on a server, PC or mobile device.

How does encryption work when transmitting a message?

In the simplest terms, sending a message using encryption is like sending the message in a scrambled code. The only way to decode the message is to have the correct key to unlock the scrambled code. For those that do not have the correct decode key, the message looks like a random string of letters, numbers and characters, making the message unreadable.

Encryption is very important (and even required by law) if you are transmitting sensitive information, such as personally identifiable information or organizational financial or health-related information. Encrypting your data transmissions is a key step to making sure unauthorized people are not allowed to access or view the information.

Be aware... In some business sectors, new regulations and standards require you and your organization to ensure sensitive and personally identifiable information sent over public networks (like the Internet) is **always** encrypted.

Awareness Vault

MOAT empowers organizational Administrators to upload organization specific and customized policies, procedures, plans, standards, training and etc. into the Awareness Vault for User training and acknowledgements. All Users can access their Awareness Vault any time and as needed to review any document assigned to them or to acknowledge documents for certification, regulatory and legal obligations. MOAT Administrators can utilize Awareness Vault tools to create T/F or Multiple Choice questions that will help ensure awareness and accountability across their entire organization.

MOAT Administrators can assign documents to one or more Departments/Groups to ensure secure access to only those Users who need to see it. Documents can be designated as part of the Users' annual certification requirements or required one-time/as needed or not required. Documents in the Awareness Vault can be updated and re-assigned as needed. Organizations can utilize the Awareness Vault as an enterprise-wide information sharing platform for compliance and internal controls for all departments (HR, IT, Risk Management, Safety, Audit, Legal, Emergency, Law Enforcement, etc.).

SEC-501 requires agencies to develop and ensure awareness for organization specific procedures. Security awareness training solutions alone fail to meet requirements defined in nine detailed sections of SEC-501 (Risk Management, IT Contingency Planning, Information Systems Security, Logical Access Control, Data Protection, Facilities Security, Personnel Security, Threat Management, IT Asset Management, etc.). The MOAT Awareness Vault equips organizations to meet these requirements, as well as other information security regulations and obligations. With the Enhanced Vault, HIPAA, FERPA and PCI-DSS training Modules are free of charge and can be placed into the Vault.

MOAT Administrators continuously rave about on-demand access to a comprehensive suite of reports to monitor User activities in real-time including: Certified Users, User Progress, Approaching Compliance, Past Due, Document Status, User Activity Log and more. Reports are also needed for compliance audits, examinations, accreditations, internal controls reviews, risk reviews, personnel performance reviews, legal due diligence and more.

TIPS/Incident Reporting/Incident Management/Prevention and Risk Management

With the Enhanced Awareness Vault, organizations can also use Awareity's internal incident reporting and incident management tools for receiving and responding to incident reports from students, employees, faculty, staff, contractors, etc. Organizations can create customized incident reporting forms for security incidents (breaches, fraud, phishing attempts, etc.), as well as safety concerns like student safety, workplace violence, threats to harm, suicide, weapons, etc. or employment concerns like personnel issues, sexual harassment, ethics, etc. Customized teams are assigned to each incident type, so only those responsible for receiving and responding to specific reports will receive notifications and have secure access to the information.

Once an incident report is submitted, all appropriate team members will be instantly notified so they can proactively respond to the incident, coordinate with other team members, document actions taken, set reminders for follow-ups, review related reports and determine the best overall responses. Comprehensive documentation provides the team members and the organization with regulatory, legal and certification reporting necessary to prevent expensive fines, lawsuits and incidents.

Surveys and Risk Assessments

Organizations can create customized surveys and risk assessments to gather critically need information from Users (employees, vendors, contractors, staff, students, third-parties, etc.) on all types of risk management topics, because organizations do not know what they do not know until they ask.

Customer Support

Users can contact support@awareity.com with any questions, saving organization valuable time and money on internal Help Desk resources. Awareity also provides comprehensive Administrator support.

MOAT/TIPS is currently equipping organizations across the country, including schools, colleges, state agencies and law enforcement to improve operational efficiencies and significantly reduce costs. TIPS was also recently selected for several national awards.

Contact info@awareity.com to learn more or to schedule an online demonstration.

"MOAT allows the Standards and Compliance Division to obtain documentation to show as a proof of compliance dealing with VLEPSC standards in order to maintain our accreditation."
- Sgt., Sheriff's Office

"We have used MOAT to fulfill state security awareness training requirements and also to require employees to be aware of any additional security responsibilities they have based on special or additional access that they are provided."
- LO, State University

"Our teachers and staff are vigilant, but you can't prevent situations you don't know about. TIPS provides us with one more way for students, teachers, parents and members of the community to alert us to potential problems - either inside or outside our schools. We can be proactive and intervene appropriately, whether it's suspected bullying, harassment or fear that a student might take their own life."
- K12 School Superintendent



Risk Innovator Award 2011



Liberty Mutual Responsibility Leader



Business Insurance Innovation Award