**Security Awareness and Training Policy**

**1. Overview**

We take protecting our organization and its data, systems, and reputation seriously. We recognize human risk as one of the top risks our organization faces. We define human risk as including accidental threats (trusted individuals making simple mistakes), negligence (trusted individuals deliberating not following policies), and deliberate threats (the malicious targeting of our workforce). In addition, leadership values not only secure behaviors but also establishing a strong security culture that contributes to the overall security and mental health of our workforce.

**2. Purpose**

To effectively manage our human risk, our security team (in partnership with other departments) will provide continuous outreach and training to all our employees and contractors. Our goal is to ensure individuals understand the risks in using today’s technology and to enable them to effectively use that technology safely and securely, both at work and at home. In addition, the security awareness program will be used to actively promote, educate, and train our workforce on all relevant security policies and procedures. The end goal is to ensure our workforce is actively exhibiting expected secure behaviors to reduce our human risk to an acceptable level. In addition, we intend to build a strong security culture that contributes to, enables, and encourages our workforce to easily exhibit secure behaviors. The overall approach of the program will use positive engagement not only to promote secure behaviors but to help create a strong, positive security culture.

**3. Scope**

This policy is applicable to all individuals (senior leadership, employees, and contractors) who have an organization email address and/or access to organizational systems or information.

**4. Policy**

4.1 Training

All employees are required to take and successfully complete security training, usually in the form of online computer-based training (CBT) or instructor-led training (ILT), within the first 30 days of employment. They are then required to retake and complete the training on an annual basis. All contractors or vendors with an organization email address or access to company data are required to take the same training (or equivalent) before they can gain access to our data or our systems and to continue to train on an annual basis if they are retained for longer than 1 year.

However, we recognize that annual training alone is not enough to secure our workforce and ultimately build a strong security culture. In addition to annual training, our security team will actively provide security communications, engagement, and reinforcement training throughout the year, to include the following:

* Monthly phishing simulations
* Annual security surveys
* An active online forum where our workforce can interact with and ask the security team questions or learn more about security, expected behaviors, and/or our security policies
* Additional training materials such as newsletters, infographics, microvideos, digital signage, tip sheets, and podcasts
* Special events such as guest speakers or scavenger hunts
* Knowledge assessments and quizzes to test knowledge retention and comprehension
* Periodic unscheduled awareness assessments to ensure compliance with the training
* Feedback surveys to improve our security awareness training and education program

Training completion and results are maintained in personnel files as part of the permanent record. Certain passing requirements and/or additional training may be required for specific personnel based on their work roles and/or risk profiles.

4.2 Role-Based Training

Certain high-risk roles, departments, or regions may require additional or specialized training. For example, the developer team may be required to take additional secure software development training or the IT staff may be required to take additional privileged access or cloud-based training. Specialized role-based training can be mandated based on risk to the organization.

4.3 Ownership and Responsibilities

The security team will dedicate at a minimum one full-time individual to the role of security awareness and education. This individual will report directly to the CISO. This individual’s responsibility is to identify, prioritize, and manage our organization’s human risk through outreach, engagement, and training of our workforce. This individual will be expected to actively partner and work with members of the security team and other departments, including communications, marketing, legal, privacy, and human resources, to facilitate outreach and training efforts.

4.4 Updating

The awareness program and corresponding training will be actively reviewed and updated on an annual basis, to include reviewing not only the human risks being addressed but the modalities and methods used for engagement, communication, and training and the metrics framework used to measure impact.

4.4 Training Records and Measurements

Training events, participation and completion, engagement of the workforce, and key behaviors and the risks they manage will all be maintained and tracked for both compliance purposes and to better manage the overall program.

**5. Enforcement**

Any individual who fails to take the required training, who continually fails periodic assessments, or consistently demonstrates a risk to the organization may be interviewed by the individual’s supervisor or security team to help better understand why. Additional training or security controls may be required. In rare or exceptional cases, the individual could be subject to disciplinary action, up to and including termination of employment.

**6. Definitions and Terms**

None

**8. Revision History**

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| December 2021 | Security Awareness Team | Separated out from the Acceptable Use Policy (AUP) and converted to new format. |