Cybersecurity Awareness Program

Cybersecurity risk is a significant organizational concern for Arete. To sustain current operations and continue to grow the company, Arete must implement robust measures to protect the company from undue cybersecurity risk and secure specific cybersecurity liability insurance. To secure this insurance, Arete must provide evidence of regular and robust cybersecurity training and simulations completed by all employees, as well as implement corrective or remediation actions when employees' actions present a significant risk.

Arete's program includes the implementation of mandatory training and regular simulation campaigns administered on our behalf by a third-party provider. The following actions will be implemented (collaboratively by an employee's supervisor and the provider) in each of the scenarios outlined, for employees who have been working with Arete for 60 days or longer.

Note

- The 12-month period for each scenario is a rolling, not calendar, period.
- The third-party provider will contact the President with the outcomes of each training and simulation campaigns. The President will reach out to relevant supervisors with next steps as required.
- Employees who have been employed less than 60 days with Arete will be expected to participate in all mandatory training and will be subject to simulation campaigns but will be provided a temporary grace period from the actions noted below.

Training

Scenario 1

Employee failed to complete assigned mandatory training within the 30-day period.

Action: Employee's supervisor will meet with the employee within five working days to review and discuss the lack of completion, reiterate the importance of cyber vigilance and re-issue the training, to be completed within two business days of receipt. The supervisor will confirm in writing the date this meeting and training were completed on the employee's Human Resources (HR) file (i.e., Stage 1 Warning, as per Section 3.10) and will provide this written confirmation to the President for tracking purposes within appropriate organizational risk records.

Scenario 2

Employee failed to complete assigned mandatory training within the 30-day period.

Action: Employee's supervisor will meet with the employee within five working days to review and discuss the lack of completion, reiterate the importance of cyber vigilance and re-issue the training, to be completed within two business days of receipt. The supervisor will create a formal performance improvement plan (i.e., Stage 2 Warning, as per Section 3.10), place a copy of the plan on the employee's HR file and manage performance of the plan in accordance with Section 3.10. The supervisors will provide written confirmation of these actions to the President for tracking purposes within appropriate organizational risk records.

Simulation Campaigns

Scenario 1

Employee failed one simulation campaign over the 12-month period (i.e., either clicked the link or clicked the link and provided credentials).

Action: Employee's supervisor will meet with the employee within five working days to review and discuss the campaign and reiterate the importance of cyber vigilance. The supervisor will confirm in writing the date this meeting took place and will provide this written confirmation to the President for tracking purposes within appropriate organizational risk records.

Scenario 2

Employee failed two simulation campaign over the 12-month period (i.e., either clicked the link or clicked the link and provided credentials).

Action: Employee's supervisor will be notified and will coordinate a one-on-one session between the employee and a representative from the third-party provider within five to seven working days to debrief the simulation with the employee, reiterate cyber vigilance best practices and provide additional mandatory trainings (i.e., once per month for the next three months). The supervisor will document the date this meeting was completed on the employee's HR file (i.e., Stage 1 Warning, as per Section 3.10) and will provide this written confirmation to the President for tracking purposes within appropriate organizational risk records.

Scenario 3

Employee failed three simulation campaign over the 12-month period (i.e., either clicked the link or clicked the link and provided credentials).

Action: Employee's supervisor will be notified and will develop and present a formal performance improvement plan (i.e., Stage 2 Warning, as per Section 3.10) within five to ten business days, which includes a robust remediation training plan to address gaps (i.e., mandatory training a minimum of once a month for the next six months) and notice that the employee will be subject to additional phishing simulations (once a month for the next three months). The supervisor will place a copy of the plan on the employee's HR file, manage performance of the plan in accordance with Section 3.10 and provide written confirmation of these actions to the President for tracking purposes within appropriate organizational risk records.