Phishing Corrective Action Guidelines (Revised 2/1/24)
Applicable to Corporate Goal Phishing Simulations (Currently Level 3*)

Training & Failure Notifications	User is auto-enrolled in web-based training immediately after failing a phishing simulation[1] Direct leader andVP of Operating Unit will receive phishing status report each quarter of user's failures					
	1st Failure	2nd Failure	3rd Failure	4th Failure	5th Failure	Failure Reset
SCE/EIX Employees	User will receive a coaching session from their direct leader[2]	Baseline: User will receive a verbal warning	• User must complete instructor-led training and a cyber "buddy" is assigned through Cybersecurity Awareness • Enhanced security controls may be applied (where applicable) • Baseline: written warning and a notification that future failures may result in disciplinary action up to and including termination	• User must complete instructor-led training • Enhanced security controls may be applied (where applicable) • Baseline: final written warning and a notification that 5th failure may result in disciplinary action up to and including termination	Baseline: Termination of employment	Once a user goes 12 consecutive months without a failure on corporate goal simulations, their record will reset to zero.[3] Leader to consult with Employee/Labor Relations for corrective action recommendations to ensure consistency with these guidelines.
Supplemental Workers (SW)	• SW is auto-enrolled in web-based training immediately after failing a phishing simulation. • SCE direct leader and VP of Operating Unit receive a phishing status report each quarter of SW's failures. • At each phishing failure, the SCE leader of the SW will be notified to contact the vendor and inform them that if there is a fourth failure, the assignment will be terminated.					

Physical Security and Cybersecurity Policy (version 9, effective May 12, 2023): "Clicking on suspicious links, opening suspicious attachments, or providing login credentials in response to suspicious emails, links or attachments may result in corrective action, including up to termination of employment." The Company conducts simulated phishing exercises based on current phishing tactics, which are subject to the Company's Phishing Corrective Action Guidelines.

1. Assigned training will come from CyberAware@sce.com with a link to Success Factors. Training is only available for 30 days.
2. The coaching template is in the Leaders Toolkit (My Staff > Managing Essentials > Leaders Toolkit). Leaders are responsible for properly documenting and maintaining records of discussion.
3. Upon 1st failure, if user fails another Corporate Goal phishing simulation (within a 12-month period), it will be recorded as a second failure and the 12-month window for resetting starts again.
   Example: 1st failure in January and 2nd failure in June – user must not fail another Corporate Goal phish simulation until the following June. Once the user's record resets to zero, the next failure will start as the 1st failure.

*Phishing Simulation Difficulty Levels

Attributes may include:

Level 1: Suspicious domain/links, 3+ grammatical errors, no business relevance, generic greeting
Level 2: Suspicious domain/links, 1-2 grammatical errors, some business relevance, personal greeting
Level 3: Suspicious domain/links, 0-1 grammatical errors, requests for login information, high business relevance, personal greeting, impersonation of business units (HR, Service Desk, etc.)
Level 4: Suspicious domain/links, 0 grammatical errors, requests for login information, highest business relevance, personal greeting, spoofed company domains, employee specific references (e.g., your leader's name)