Policy number	Title:	Effective Date:
<your ID format>	SECURITY AWARENESS TRAINING POLICY	<your date format>

REFERENCE **<this shows the following relevance should all the policy content be followed>**

- CIS C14, NIST CSF PR.AT-1, ID.AM-6, ID.GV-1

SUPPORTING DOCUMENTS

- **<This is a contents link space for any related documentation.>**

CONTENTS

PURPOSE

A modern cybersecurity program cannot be put into place without ample attention given to security awareness training. This includes designing a robust program that is properly developed, implemented, and updated. This Security Awareness Training Policy provides the processes and requirements for this program.

RESPONSIBILITY

The IT business unit has the primary responsibility for planning, developing, and updating the cybersecurity awareness training program. The education aspect may be performed by the IT business unit or others they deem fit to provide the training. With that said, all employees and users have a responsibility to implement the concepts taught within the security awareness program.

POLICY

DEVELOP

- A program for performing security awareness training must be established.
- All new members of staff must complete approved security awareness training prior to, or at least within 30 days of starting employment at **<company name>**.
- All personnel must complete the annual security awareness training.
- All personnel must be provided with, acknowledge that they have received, and agree to adhere to the IT Acceptable Use Policy.

EDUCATE

- Users must be trained on how to recognize social engineering attacks.
- Users must be trained on best practices for authentication in the enterprise.
- Clear screen and clean desk best practices must be included in the training.
- Users must be trained on the causes of unintentional data exposure in the enterprise.
- Users must be trained on how to recognize and report security incidents.
- Users must be trained on how to identify and report if their enterprise assets are missing security updates.
- Users must be trained on the dangers of connecting to and transmitting enterprise data over insecure networks.

UPDATE

- The content of the security awareness training program must be reviewed and updated annually, or when significant changes to the enterprise occur.

COMPLIANCE

In the event of failure to comply with any IT Policy, **<company name>** may at its sole discretion:

- Restrict or terminate a user's right and ability to use or access any or all **<company name>**'s IT systems and facilities.
- Withdraw or delete any data that contravenes this policy.
- Any disciplinary action arising from a breach of this policy shall be dealt with in accordance with the **<company name>** Disciplinary Policy.

DATE ISSUED/DATE REVIEWED

Date Issued:	
Date Reviewed:	