Cybersecurity User Awareness Training

SIT374 Team Project A

*Redback Operations*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Modified By** | **Approver** | **Date** | **Changes made** |
| 1 | Jamison Begley |  |  | Document Creation |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

*​*

Contents

[Purpose 4](#_Toc165030424)

[Introduction 5](#_Toc165030425)

[What is user awareness training? 5](#_Toc165030426)

[What is the purpose of user awareness training? 5](#_Toc165030427)

[Why Do We Follow This Training? 6](#_Toc165030428)

[Risks of Non-Compliance 6](#_Toc165030429)

[Advantages of Training 6](#_Toc165030430)

[What Does This Training Cover? 7](#_Toc165030431)

[How Often Should This Training Be Covered? 7](#_Toc165030432)

[Where Can This Training Be Accessed? 7](#_Toc165030433)

# Purpose

The purpose of this User Awareness Training document is to define the standards that must be in place and followed for the training and upskilling of our employees. The document will outline any training modules that must be completed to not only guarantee security compliance, but to ensure employee knowledge.

# Introduction

## What is user awareness training?

User awareness training refers to the guidelines put in place by an organisation to help educate workers about the potential risks of their role and job functions. Though the awareness training typically focuses on data protection, data security and overall compliance with company policies.

## What is the purpose of user awareness training?

User awareness training serves a range of crucial functions within an organisation. Aside from educating workers about the potential risks of their job functions, it also provides employees with a range of strategies and procedures that they can follow to mitigate or resolve these risks effectively.

Through the provision of this training, not only is data security improved, but if followed correctly, there may be a significant increase in company performance and morale.

Finally, user awareness training works to minimise potential loss, and consequently, it works to foster a safe and positive working environment.

# Why Do We Follow This Training?

We follow our user awareness training as it is put in place to prevent any sort of risks that may present themselves and pose a threat to the company.

## Risks of Non-Compliance

If we did not follow our user awareness training protocols, a collective employee gap in knowledge may leave Redback Operations prone to, and susceptible of a range of attacks.

These attacks can target our sensitive data, company systems, assets, trade secrets and critical infrastructure.

In the event of an attack, if employees haven’t conducted our user awareness training, we may suffer a significant data leak and/or data loss due to a lack in knowledge of how to appropriately respond to or prevent such a thing. This data may be revealed to the public, which will hold a significant impact on the company, and its relationship with consumers, as their information may be susceptible to tampering, unauthorized disclosure, or it may be used against them.

Not only this, but the compromise of our company systems, assets, and critical infrastructure may lead to a complete loss of access, to both, our data, and our recovery systems, causing us to lose everything we have.

## Advantages of Training

Though contrary to the described risks, if employees have completed their awareness training, they will be able to respond to an attack accurately and effectively, or ultimately prevent the risk of a possible attack or data breach, securing our systems and critical infrastructure.

As a result, we, as a company can remain completely transparent with our consumers, maintaining their trust in our ability to withhold their personal information securely.

# What Does This Training Cover?

The user awareness training covers a range of topics relevant to our cybersecurity employees and their job functions,

To name a few, the training will cover an employee’s understanding and awareness of the core functions Redback Operations, our playbooks, ethics, data classification and protection procedures.

# How Often Should This Training Be Covered?

Our Cybersecurity User Awareness Training should be completed upon employment, and a refresher training should be completed every 12 months within the timeframe allocated on a designated week.

# Where Can This Training Be Accessed?

Within the company repositories, a document can be found which describes the minimum amount of acquired knowledge that an employee must have, though it is followed by a quiz that employees must earn a perfect score on to be recognized for the completion of their training.