Cybersecurity User Awareness Training

SIT374 Team Project A

*Redback Operations*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Modified By** | **Approver** | **Date** | **Changes made** |
| 1 | Jamison Begley |  | 10/05/2024 | Document Creation |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

*​*

Contents

[Purpose 4](#_Toc165378621)

[Introduction 5](#_Toc165378622)

[What is user awareness training? 5](#_Toc165378623)

[What is the purpose of user awareness training? 5](#_Toc165378624)

[Job/Role Specific Training 6](#_Toc165378625)

[Understanding Routes for Help 7](#_Toc165378626)

[Understanding Reback Operations’ Major Areas 8](#_Toc165378627)

[Understanding Data Classification 10](#_Toc165378628)

[Understanding Data Loss Prevention Strategies 11](#_Toc165378629)

[Encryption Standards 12](#_Toc165378630)

[Playbook Awareness 13](#_Toc165378631)

[Attack Playbooks 13](#_Toc165378632)

[Vector Playbooks 13](#_Toc165378633)

[In-Depth Playbook Access 13](#_Toc165378634)

[Ethics 14](#_Toc165378635)

[Ethical Standards of Redback Operations 14](#_Toc165378636)

[Ethical Requirements of Redback Operations 14](#_Toc165378637)

# 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 the importance of and reasoning for these standards and will mention any training or learning that must be undertaken by employees to guarantee security compliance.

# 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.

# Job/Role Specific Training

This training will highlight all the general training that needs to be completed to understand our safety practices and procedures within Redback Operations, though it will not deliver information related to specific jobs/roles within the organisation.

Specific job/role training will be conducted through the job itself, however this training must be completed regardless.

# Understanding Routes for Help

At Redback Operations, roles and responsibilities are broken down into sub teams, such as our “Purple Team” (Red + Blue), “Blue Team” (Secure Coding), “Green Team” (Identity and Access Management), “Yellow Team” (Governance and Policies), and our “Red Team” (Infrastructure/Other).

It is important to understand what team you, as an employee belong to, to identify what your route for help is. Each team should be familiar with their fellow team members, including their team leader – to which they should reach out to if help is required.

If the help required is based on gaps in knowledge, documentation such as policies, rules, and procedures can be found on our company repositories, such as docusaurs or Github in order to strengthen this knowledge, though if more help is required, it is best to contact a team leader.

# Understanding Reback Operations’ Major Areas

To ensure the protection of Redback Operations’ Major Areas, all users must be informed and educated on what they are, and what can be done to monitor and protect them.

The major areas of Redback Operations that need to be monitored are as follows:

* **Cloud Infrastructure** – “Monitoring the performance, availability, and security of the cloud infrastructure”. This can be monitored through the “implementation of 2-Factor Authentication”.
* **Application Performance** – “Monitoring the performance of Redback Operations’ applications”. This can be monitored through “user feedback and reviews”.
* **Resource and Usage Cost** – “Keeping track of resource usage and associate costs”. This can be done through “tools such as Datadog or Grafana… to monitor CPU usage”, alongside “budgeting practices” with “a cost-usage matrix”.
* **Security and Compliance** – “Monitoring security events, vulnerabilities, and compliance with industry standards”. This can be monitored through “regular checks on full compliance policies”.
* **Network Performance** – “Monitoring network latency, bandwidth, and traffic patterns”. This can be monitored through “real-time bandwidth measurements”.
* **Backup and Disaster Recovery** – “Monitoring backup processes and disaster recovery plans”. This can be monitored through the “administration of an automated storage backup program”.
* **User Activity and Usage** – “Monitor user activity and usage patterns”. This can be monitored through “logging mechanisms… to verify and record user authentication events”.
* **System Updates and Patches** – “Keeping track of system updates and patches”. This can be monitored through “patch management software”, to ensure that the company’s systems are up-to-date and detected vulnerabilities are actively patched.

For an in-depth guide on how to monitor the major areas of Redback Operations, please refer to the document titled “how can we monitor major areas.docx”, which can be found on our company Github repo.

*Descriptions sourced from “major\_areas\_to\_be\_monitored.docx”.*

*Solutions sourced from “how can we monitor major areas.docx”.*

# Understanding Data Classification

Understanding data classification is a pivotal point on knowledge in a user’s training, as this can help to give a gauge on the level of cautiousness and security that a user must take when recording, handling, and storing specific data.

As mentioned in our Data Classification & DLP Policy, data classification is broken down into four levels.

* **Public** refers to “data intended for public disclosure”, where confidentiality is not a top priority as the data is intended to be accessed by the public.
* **Internal Use Only** refers to “data that is not sensitive but is intended for use within the organisation”. In this case, the security is not imperative but should be considered.
* **Confidential** refers to “sensitive data that could cause harm to the organisation or individuals if disclosed. In this case, data must be carefully handled and protected from the public as the disclosure of this may cause harm to the company.
* **Restricted** refers to “highly sensitive data that if disclosed could result in significant harm or legal/regulatory non-compliance”. In this case, data must be treated with absolute care, with all safety measures in place to ensure its confidentiality and integrity.

Please refer to our “*Data Classification – DLP Policy.docx*” on our company repositories for further information.

*Information sourced from “Data Classification – DLP Policy.docx”*

# Understanding Data Loss Prevention Strategies

In tandem with Data Classification, Data Loss Prevention (will now be referred to as DLP) strategies are put in place to “ensure the safety and integrity of our data” through the deployment of “a range of safety measures and policies to accurately respond in the event of a data breach”, “proactively identify[ing], monitor[ing], and mitigat[ing] risks involved with unauthorized access, data distribution or breaches of sensitive data.

At Redback Operations, we follow seven different DLP strategies, these are as follows:

* **Data Classification** – “Data must be classified based on its sensitivity, importance, and business impact to Redback Operations”.
* **Access Controls** – “The least privilege principle must be implemented, restricting access rights to only those that directly require access to perform their job function”.
* **Watermarking Content** – “All confidential information that is integral to the company should be watermarked with “Redback Operations”, to prevent “the ability for anyone to steal any data or documentation and claim it as their own”.
* **Encryption** – “All sensitive material within Redback Operations should undergo encryption to reduce the overall business impact in the event of a data breach”.
* **Preventing Unauthorized Copies of Data** – Whilst adhering to the same standards as Access Controls and Watermarking Content, “screen-capture prevention and clipboard control should be implemented” to prevent unauthorized copies of data.
* **Content Inspection** – “Regular examination of files, documents, and automated monitoring of communications” should be conducted to ensure data security.
* **Policy Enforcement** – “There should be both automated and physical inspections on all sensitive data being transmitted or stored within Redback Operations to ensure that it follows all DLP and Data Classification Policies”.

For an in-depth description for the implementation of DLP strategies, please refer to the document titled “Data Classification – DLP Policy”, which can be found on our company Github repo.

*Information sourced from “Data Classification – DLP Policy.docx”*

# Encryption Standards

Though encryption is mentioned in our Data Loss Prevention Strategies, a larger focus must be placed onto it, as it is the governing factor that works to protect the confidentiality and integrity of our data. All encryption standards must align with our Cryptography policy.

All employees must be aware of the “Roles and Responsibilities” section within the cryptography policy – and specifically they should understand what their role is within the team.

Similarly, employees that are responsible for data transfer and data storage should understand our “Secure Protocols”, which involve using “Transport Layer Security 1.2 or higher” when **transmitting data over public networks,** opposed to “forbidden”, “insecure protocols such as SSL2, SSL3, TLS 1.0 & TLC1.1”.

Similarly, symmetric encryption must take place “for internal encryption needs, including data at rest, AES (Advanced Encryption Standard) with key sizes of 256 bits is approved”.

Alternatively, asymmetric encryption must take place “for digital signatures and key exchange mechanisms, RSA with a minimum key size of 2048 bits or ECC with a minimum key size of 256 bits are approved”.

Finally, when conducting file hashing, “SHA-256 or higher is approved for hashing operations”.

Please refer to our “Cryptography Policy.docx” on our company repositories for further information.

*Information sourced from “Cryptography Policy.docx”.*

# Playbook Awareness

Our team at Redback Operations and developing and have developed a range of incident response “playbooks” which work to educate users on the risks and attacks that the company may face – an example of this being for our “phishing incident response playbook”. Though this section will brief over our playbooks, what their purpose is, and how to access them.

Each playbook is broken down into seven sections, these being “preparation”, “identification”, “notification”, “containment”, “eradication”, “recovery”, and “post-incident” responses, each unique to the specific circumstances.

## Attack Playbooks

These playbooks outline how to prepare for, identify, eradicate, and recover from a range of attacks on the company’s data and systems.

The attack playbooks account for the following attacks: Denial of Service (DoS), Phishing, Ransomware, Malware, Data Breach, and Industrial Control System Compromise Playbook.

The attack playbooks hold a heavy significance on preparation for an attack, with the implementation of a robust range of preparation strategies, such as backups, access controls, monitoring tools and general employee response training. Though if an attack is successful, we conduct post-incident analysis and reviews to looks for areas to improve on, to prevent recurrence of an attack.

## Vector Playbooks

These playbooks outline a range of ways to identify, eradicate, and recover from a range of vectors that may cause an unauthorized intrusion to the company’s systems.

The vector playbooks account for the following vectors: External/Removable Media Vectors, Attrition Vectors, Web Vectors, Email Vectors, Supply Chain Interdiction Vectors, Impersonation Vectors, Improper Usage Vectors, and Loss/Theft of Equipment Vectors.

The vector playbooks primarily focus on authentication measures, regular system checks and filtering to prepare for any of these intrusion attempts. Though if any of these vectors invade our servers, our post-incident response is to always review and analyse our current measures to adjust for any gaps or vulnerabilities to prevent recursion of the intrusion.

## In-Depth Playbook Access

An in-depth read-through of the playbooks, outlining steps for preparation, identification, notification, containment, eradication, recovery, and post-incident responses can be found within the company’s repos – either through Github or Docusaurs.

# Ethics

Ethics refer to the “moral principles that govern a person’s behaviour or the conducting of an activity” (Oxford Languages). They are put in place to ensure the compliance of relative security principles that are in place within an organisation.

An ethics framework is a staple in any organisation, as it governs the organisation’s values, purpose, and principles on how they conduct their business matters to keep a transparent and trustworthy relationship with their consumers.

From a cybersecurity stance, ethics refers to our collection, storage, and transmission of sensitive information. Though compliance with these ethical standards and requirements must always be followed, as non-compliance can lead to significant impacts on the company’s integrity and trust with its consumers.

## Ethical Standards of Redback Operations

At Redback Operations, we follow a range of Ethical Standards to guarantee our trust and transparency with our consumers, there ethical standards are as follows:

**Transparency and Consent**

All forms of data collection must be briefed with consumers, and they must provide full, written consent.

This consent must outline what data is being collected, how it will be collected, how it will be stored, how it will be used, and any risks associated with potential data breaches, unauthorised access, and data loss.

**Confidentiality**

All information classified as “Internal Use Only”, “Confidential”, or “Restricted” must have the correct access controls applied to their accessibility. Building onto this, encryption standards must be put in place to keep information confidential, even in the event of a data breach.

**Privacy**

Data collected from consumers must remain private to both, the outside world, and our employees. To do this, data anonymity must be utilised to protect the privacy of our consumers, so their personal data cannot be traced back to them in the event of a data breach.

**Secure collection, storage, and transmission of data**

Adhering to our cryptography policy, and general cryptography standards, data must be securely collected and stored. Similarly, data must be securely transmitted – further explanation on how to do this can be sourced from our cryptography policy.

**Data Usage**

To monitor data usage, data minimalization can take place, by limiting the data that we collect from our consumers to only be data that we require for the function of our work. For example, personal data such as addresses and other sensitive, unrelated information should not be collected as that information is not required for our job function.

**Compliance**

Ultimately, all Redback Operations Policies and Procedures – such as this training and other policies must be actively adhered and complied to, guaranteeing the overall company security and protection, while ensuring our transparency and relationship with our consumers.