DLP & Data Classification Implementation Plan

SIT374 Team Project A

*Redback Operations*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Modified By** | **Approver** | **Date** | **Changes made** |
| 1.0 | Jamison Begley |  | 1/8/24 | Document Creation |
| 1.1 | Jamison Begley |  | 16/8/24 | Updated Watermark Section, Fixed Grammar |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

*​*

Contents

[1. Purpose 4](#_Toc173749693)

[2. Data Loss Prevention 5](#_Toc173749694)

[Access Control Levels 5](#_Toc173749695)

[Watermark 6](#_Toc173749696)

[Encryption Applications 6](#_Toc173749697)

[Content Inspection 6](#_Toc173749698)

[Adherence to Regulatory Requirements 6](#_Toc173749699)

[3. Data Classification 7](#_Toc173749700)

[4. Conclusion 8](#_Toc173749701)

*​*

*​*

*​*

*​*

*​*

​**​**

# Purpose

The purpose of this DLP & Data Classification Implementation Plan is to outline the measures and considerations that need to be put in place in order to ensure the compliance and ease of implementation of our DLP & Data Classification Policies at Redback Operations. This document should be regularly referred to and audited to ensure overall compliance.

# Data Loss Prevention

To easily implement our Data Loss Prevention Policies/Principles, the following measures should be identified and adhered to.

## Access Control Levels

Access control levels need to be broken down into a hierarchy – where those with more responsibility and motion within the company should have more access than those who are working at a lower title/rank. Access control level should be broken down, and implemented as follows:

**Company Leader**

The company leader should have complete, overall access to all forms of documentation, work, and projects, as they oversee all operations within Redback Operations

**Team Leader**

The team leaders (for each project) should have complete access to all work, projects and documentation that directly relates to their team. For example, the Cybersecurity team leader should have complete access to all forms of work, documentation and projects directly associated with the cybersecurity team, and should only be able to access publicly available information for the other projects/teams.

**Sub-Team Leader**

Sub-Team leaders, such as those for the GRC team, Red Team, Blue Team, etc., should only have direct access to the work directly associated with their sub-team, as they oversee all the work done by their respective sub-team and should only be able to access publicly available information for the other Sub-Teams.

**Team Member**

Team members should only have access to the work, documentation and projects that they are directly involved in, though work may be shared within sub-teams if appropriate and non-restricted. Aside from their own work and work shared with them, team members should only be able to access publicly available information associated with the company, and its current/past projects.

In defining these Access Control levels, we can further prevent unauthorized copies of data by only allowing those with sufficient access levels to be able to access and modify our documentation.

## Watermark

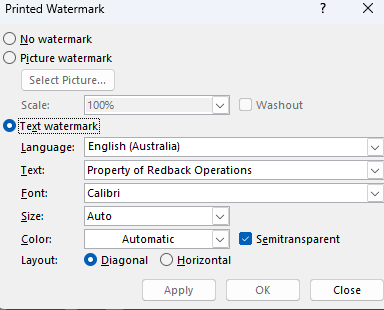
The Redback Operations watermark must be included in all forms of work, documentation and projects to ensure the integrity of our data – this watermark is available to all levels of employees.

The watermark consists of a single form, which can be implemented in Microsoft suite applications, such as Word or PowerPoint. The watermark should be a string of text spanning from diagonal corners labelled “Property of Redback Operations”.

**How to insert our watermark:**

In a word document, in the DESIGN tab > select WATERMARK > select CUSTOM WATERMARK > select TEXT WATERMARK > type “Property of Redback Operations”.

The following screenshot shows the settings for the watermark:



## Encryption Applications

In reference to our Cryptography policy, SHA-256 or higher is required for our hashing operations, and TLS 1.2 or higher must be used for data transmission, and the AES (Advanced Encryption Standard) with key sizes of 256 must be adhered to. As mentioned in the cryptography implementation plan, services such as ‘VeraCrypt’, ‘BitLocker’, ‘Nord Locker’ or ‘AxCrypt’ can be implemented to ensure our data encryption and security aligns with our Cryptography policy.

## Content Inspection

Content inspections for work that team members produced must be done by the respective team/sub-team leaders. Content inspections should be regularly conducted on files, documents and projects to ensure that no restricted information is set to be released to unauthorized persons.

Automated email monitoring services should be implemented to alert or block emails that violate company policies, or the confidentiality and integrity of our data. An example tool that can be implemented is ‘Teramind’s “Employee Email Monitoring” solution. This automatically scans through mail that is sent and received, alerting our DLP security team in the event of unauthorized information being sent through email. Once this alert is received, our DLP team can take action to remove the email, and the individual who sent the message can be dealt with accordingly.

## Adherence to Regulatory Requirements

Regular audits must take place bi-monthly to ensure the complete compliance with each Data Loss Prevention and Data Classification policy and its respective implementation plan. These audits must have employees re-familiarise themselves with our policies and procedures and ensure compliance.

# Data Classification

To easily implement our data classification policy and practices, data must be classified based on sensitivity, importance and business impact. This can be done as follows:

* ***Public****:* Data intended for public disclosure. Encryption is not required for public data, but best practices for integrity should still be applied.
* ***Internal Use Only****:* Data that is not sensitive but is intended for use within the organization. Basic encryption controls are recommended to prevent unauthorized disclosure.
* ***Confidential****:* Sensitive data that could cause harm to the organization or individuals if disclosed. Encryption in transit and at rest, using industry-standard algorithms and key strengths, is required.
* ***Restricted****:* Highly sensitive data that, if disclosed, could result in significant harm or legal/regulatory non-compliance. Strong encryption, both in transit and at rest, with strict access controls and key management procedures, is mandatory.

(Directly sourced from ‘Cryptography Policy’ & ‘Data Classification – DLP Policy’)

# Conclusion

To conclude, the implementation of our Data Loss Prevention and Data Classification Policies can be done by complying with the above information.

This plan should be regularly reviewed and audited to ensure compliance in all areas (this audit can be done every quarter).

The overall compliance and implementation of this plan is pivotal for the security and protection of data within Redback Operations.