DLP & Data Classification Policies

SIT374 Team Project A

Redback Operations

Version	Modified By	Approver	Date	Changes made
1	Jamison Begley		16/04/24	Document Creation

Table of Contents

Contents

1. Purpose 4
2. Data Classification 5
2.1 - Sensitivity 6
2.2 - Importance 6
2.3 - Business Impact 7
2.4 - Data Classification Summary 8
3. DLP Policies 9
3.1 - Data Classification 9
3.2 - Access Controls 9
3.3 - Watermarking Content 9
3.4 - Encryption 10
3.5 - Preventing Unauthorized Copies of Data 10
3.6 - Content Inspection 10
3.7 - Policy Enforcement 10
4. Conclusion 11

1. Purpose

The purpose of this DLP & Data Classification Policy is to ensure that all possible protective measures are followed to ensure the integrity, confidentiality and overall safety of Redback Operations' assets and sensitive information. Though the measures within this policy should be regularly audited and checked for compliance to guarantee the company's digital safety.

2. Data Classification

To ensure the safety and integrity of our data, we must deploy a range of carefully illustrated Data Classification Policies, which must be adhered to, to protect sensitive information in the event of a data breach.

Data Classification Policies are designed to categorise and prioritise data based on factors such as its sensitivity, importance, and its impact on the business. This categorisation can influence the appropriate storage, encryption, and access requirements for different types of data, ensuring the protection of sensitive information. Though these Data Classification policies must work in tandem with our DLP (Data Loss Prevention) policies, which are designed to identify, monitor, and mitigate risks to effectively safeguard our data.

This report will examine and explain the principles that Redback Operations must follow to effectively categorise and classify their data, ensuring the confidentiality and integrity of our data assets.

2.1 - Sensitivity

Sensitivity refers to the level of confidentiality or privacy associated with the data, indicating how critical it is to protect against unauthorized access or disclosure. Data that may be considered sensitive includes all types of personally identifiable information, such financial information, records, customer information (names, addresses, etc.). Sensitive information like this must be classified as somewhat restricted information, where only those required to access it, can do so. This can be done through the DLP policy of Access Controls.

Alternatively, non-sensitive data refers to data that does not pose any significant risks or impacts if unauthorized parties access it. Information that may be classified as non-sensitive include public business information, such as publicised business trends, general contact information or press releases. Additionally, non-identifiable data, such as anonymous customer feedback or statistical reports can also be classified as non-sensitive.

Though sensitive data must be treated as a top priority for safety, meaning access controls, encryption and proper storage of this data must take place.

2.2 - Importance

Importance refers to the direct or significant of data to the business' operations, strategic objectives, or regulatory compliance requirements. Data that may be considered important include customer databases, the company's intellectual property, business continuity documents (for future projects/campaigns) and regulatory compliance documents. Additionally, business contingency and emergency response plans must be categorised with high importance, so the documentation is easily accessible in the event of an emergency.

On the other hand, data that may be considered non-important typically includes information that is not directly relevant or critical to the business. For example, outdated data, outdated data trends, non-strategic business information, such as general industry news and general employee training information.

Ultimately, data that is considered highly important must be treated with absolute care to ensure the business' integrity and continuity.

2.3 - Business Impact

Business Impact refers to the potential consequences that could result from the loss, compromise, or unauthorized access of data, including financial losses, reputational damage, and operational disruptions. Data that may be classified as a high business impact involves any critical set of data to the company, such as customer/employee personal information, financial forecasts, and business continuity plans.

Data classified to have a high business impact if compromised should be treated with the highest level of care, meaning secure backups must be created on top of the already secure DLP policies.

On the contrary, data that may be classified as having a low business impact if compromised may include outdated marketing materials, redundant/old data, employee training materials, non-sensitive employee feedback.

Though data may be classified to have a low business impact if compromised, it still should be adequately protected and taken care of, as over time the data may eventually be considered to have a high business impact if its context or business strategies change.

2.4 - Data Classification Summary

Adhering to the previous categories, data can be classified amongst four levels: Public, Internal Use Only, Confidential, and Restricted.

- ***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.

To conclude, though all unreleased data must be protected from the public eye, data that may be considered to have a higher value to the company (sensitivity, importance, business impact) should be firmly treated with the company's DLP policies, such as proper storage, encryption, backups, and internal access controls to help mitigate any potential breaches of data within RedBack Operations

3. DLP Policies

To ensure the safety and integrity of our data, we must deploy a range of safety measures and policies to accurately respond in the event of a data breach.

DLP policies are designed to proactively identify, monitor, and mitigate risks involved with unauthorized access, data distribution or breaches of sensitive data. Though these DLP (Data Loss Prevention) policies must work in tandem with our Data Classification policies, which categorise data based on its importance and sensitivity to the company. When these are aligned and our ISMS are adhered to, a comprehensive approach can be taken to ensure the safety and protection of our data assets.

This report will examine and explain the principles, strategies, and implementation of DLP policies within Redback Operations. By adhering to all policies, we can boost our defence against data breaches and data loss, thus ensuring the integrity of our data assets.

3.1 - Data Classification

Adhering to the Data Classification Policy (listed above), data must be classified based on its sensitivity, importance, and business impact to RedBack Operations. Data is classified by three levels: Public, Internal Use Only, Confidential and Restricted. Data that is classified as “restricted” and “confidential” must be treated with absolute care, and all protection and prevention measures possible (as listed in this document) must take place to ensure the protection and integrity of the data. Though the “public” and “internal use only” levels still must be treated with a high level of care, despite not being as sensitive or important to the company.

3.2 - Access Controls

Access controls must be established to ensure the protection of sensitive data. The least privilege principle must be implemented, restricting access rights to only those that directly require access to perform their job function. Additionally, role-based access controls can be implemented for team-related work, assigning the same access permissions to a group of people, meaning those with the same assigned role can access the same levels of information. By doing so, sensitive, and important data can therefore be protected through the limitation of access.

3.3 - Watermarking Content

All confidential information that is integral to the company should be watermarked with “RedBack Operations”. This prevents the ability for anyone to steal any data or documentation and claim it as their own as the “RedBack Operations” branding will be visible across the entire document. This also enables the ability to track any potential data breaches if any copyrighted information of RedBack Operations is found online.

3.4 - Encryption

All sensitive material within Redback Operations should undergo encryption to reduce the overall business impact in the event of a data breach. Data encryption must be applied to all sensitive data while in storage and in transit. Though only those with the correct access controls should have access to information on how to decrypt the data, limiting the access of the encrypted data to only those that are required to use it.

Further encryption methods and strategies are listed in our cryptography policy.

3.5 - Preventing Unauthorized Copies of Data

Tying in with Access Controls and Watermarking Content, to prevent unauthorized copies of data, access controls must be in place to ensure only those who are trusted with sensitive material can access it, and if there were to be copies made, it will have a Redback Operations watermark across the entire document or string of data.

Moreover, screen-capture prevention and clipboard control should be implemented to both, prevent the possibility of a screen recording/screenshot or to prevent a clipboard copy of the data.

3.6 - Content Inspection

Content inspection involves regular examination of files, documents, and automated monitoring of communications (internal/external), such as emails to detect any sensitive or unauthorized information that plays a pivotal role to Redback Operations.

Automated monitoring through key word, pattern, or file type scans should take place to ensure that this sensitive or unauthorized data is not published or released to those without authorization. If this is detected, systems should be in place to either block or destroy the content being transmitted to therefore prevent data leaks.

3.7 - Policy Enforcement

Policy Enforcement acts as an overseeing body for all DLP Policies in Redback Operations. To adhere to this, 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.

Moreover, regular audits can take place to assess how effective the policies regarding DLP and Data Classifications are, and changes can be made to actively strengthen these policies to ensure a safer systematic environment.

4. Conclusion

To conclude, if all DLP and Data Classification policies that are listed in this document are always adhered to, the safety and integrity of data collected and stored by Redback Operations is guaranteed.

Though regular audits should take place to actively review all policies being followed, to counteract emerging technologies and potential risks that may threaten our data.