Security Policy Report: Access Control to Google Drive Applying the Principle of Least Privilege

Date: October 4, 2024
Prepared by: [Name of Security Officer]
Company: TechCorp Solutions

1. Introduction

Google Drive is commonly used at TechCorp Solutions to store, share, and collaborate on work documents. However, without proper control, it can become a source of data loss or unauthorized access risks.
This report proposes a security policy that limits and controls the use of Google Drive by applying the Principle of Least Privilege, ensuring that employees only have access to documents necessary for their job functions.

2. Data Classification

To improve the management of permissions and document access on Google Drive, TechCorp Solutions classifies its data as follows:

1. **Public Documents:** General company information accessible by any employee.
2. **Internal Documents:** Confidential information accessible only by authorized personnel.
3. **Sensitive Documents:** Highly confidential data (contracts, legal agreements, financial data) restricted to executives or authorized personnel under strict necessity.

Proper data classification on Google Drive is essential to define access levels and share documents only with authorized personnel.

3. Access and Control (Applying the Principle of Least Privilege)

In line with the Principle of Least Privilege, access to Google Drive will be managed as follows:

- **Restricted Access:** Employees will have access only to the documents and folders needed for their daily tasks. General access to sensitive folders will be avoided.
- **Permission Review:** Access permissions to Google Drive files and folders will be reviewed quarterly to ensure that only active and authorized personnel retain access.
- **Temporary Access:** When temporary access to sensitive documents is required, it will be granted through formal authorization and removed once the project or task is completed.
- **Limited Editing Permissions:** Only direct supervisors will have editing permissions. Other employees may have read-only access if necessary for their roles.

4. Monitoring and Auditing

A monitoring and auditing policy will be implemented to detect unauthorized access and misuse of Google Drive:

- **Activity Logging:** Google Workspace features will be used to log and monitor who accesses which documents, when, and what actions are taken (editing, downloading, sharing).
- **Security Alerts:** Automatic alerts will be configured to detect and notify the security department when sensitive documents are shared outside the organization or inappropriate access permissions are granted.
- **Regular Audits:** Quarterly audits will be conducted to review access to sensitive documents and detect potential breaches of security policies.

5. Data Leakage Prevention

To prevent the leakage of sensitive data from Google Drive, the following measures will be applied:

- **Disable Sharing with Anyone:** The option to share files or folders with "anyone with the link" will be disabled by default for documents classified as sensitive.
- **Controlled Sharing:** Sensitive documents can only be shared with employees or pre-approved external partners, and access will be controlled through read-only permissions, without download or copy options.
- **Tag Protection:** The most sensitive documents will be protected with tags such as "Confidential" or "Internal Use Only," and they can only be downloaded with special permissions.

6. Education and Awareness

It is crucial for employees to understand the importance of security policies when using Google Drive:

- **Mandatory Training:** Quarterly training sessions will be conducted to ensure employees are aware of Google Drive usage policies and how to securely handle sensitive documents.
- **Risk Awareness:** During the training sessions, examples of common incidents related to the misuse of Google Drive (such as accidentally sharing documents with unauthorized third parties) will be presented, along with best practices to avoid them.

7. Conclusion

Properly applying the Principle of Least Privilege in the use of Google Drive, along with a well-defined security policy, will ensure that TechCorp Solutions protects its most sensitive information and minimizes the risks of unauthorized access or data loss.