Cloud Data Classification Policy (AWS)

Purpose: To ensure sensitive data in cloud storage is appropriately labeled and protected.

Policy:

- All data stored in AWS S3 must be classified as Public, Internal, or Confidential.
- S3 bucket policies must reflect access rules for each classification.
- Encryption is required for all Confidential data.
- Bucket names must include classification tags (e.g., finance-confidential-2025).
- Monthly audits will be conducted via AWS Config rules.

Owner: Cloud Compliance Manager

Approved: 5/30/25