**Lab 2 Title:**

**Securing Data Across Cloud Service Models Using AWS Free Tier**

**Course: INFO50166 – Data Security and Compliance**

**Total Points: 50**

**Duration: Approx. 1.5 to 2 hours**

**Pre-requisites: AWS Free Tier account, basic knowledge of IAM, EC2, and S3**

## Lab Objectives:

1. Understand security responsibilities in IaaS, PaaS, and SaaS.
2. Apply IAM best practices and encryption in AWS.
3. Explore the shared responsibility model.
4. Reflect on real-world cloud security incidents.
5. Practice the Zero Trust model using AWS tools.

## Lab Submission Requirements:

Submit a Word or PDF document containing:

1. Screenshots of each setup step (IAM, EC2, S3, IAM Identity Center, audit log).
2. Answers to all reflection questions.
3. 2–3 sentences summarizing what you learned about securing cloud services.

## Part 1: Understanding and Implementing IAM (10 points)

**Tasks:**

1. Log into AWS Free Tier and navigate to IAM.
2. Create a user with programmatic access.
3. Assign the AmazonS3ReadOnlyAccess policy.
4. Enable MFA for the user.
5. Test access via AWS CLI.

**Reflection Questions (2 points):**

- Why is MFA important even for read-only access?

- What could happen if you assigned full access instead?

**Part 2: Securing IaaS – Launching a Secure EC2 Instance (10 points)**

**Tasks:**

1. Launch a **t2.micro** EC2 instance (Amazon Linux).
2. Configure a custom security group:
    - Allow SSH (port 22) from your IP only.
    - Block all inbound except SSH.
3. Connect to the instance using SSH.
4. Enable basic firewall using ufw.

**Reflection Questions (2 points):**

- How does the EC2 firewall configuration reflect IaaS security?
- What happens if you open all inbound ports?

**Part 3: Securing Data in S3 (10 points)**

**Tasks:**

1. Create an S3 bucket named secure-data-demo-<yourname>.
2. Upload a sample text file (e.g., sensitive-info.txt).
3. Enable default encryption (SSE-S3) on the bucket.
4. Create a bucket policy to block public access.

**Reflection Questions (2 points):**

- What are the consequences of not enabling encryption on S3?
- Why is public access blocked by default in modern S3?

**Part 4: Shared Responsibility & Zero Trust Concepts (10 points)**

**Tasks:**

1. Open AWS IAM → Identity Center → Create and assign a permission set with least privilege access.
2. Review the Shared Responsibility Model in AWS documentation.
3. Simulate a Zero Trust scenario by:

- Creating a role with limited access.
- Assigning the role to a federated user using IAM Identity Center.

**Reflection Questions (2 points):**

- In your EC2 and S3 setups, what are your responsibilities vs. AWS's?
- How does Zero Trust differ from traditional perimeter-based security?

**Part 5: Real-World Incident Simulation & Response Plan (10 points)**

**Tasks:**

1. Research the Capital One 2019 breach and list what went wrong.
2. On your EC2 instance, simulate log creation with:
3. sudo yum install -y audit
4. sudo auditctl -w /etc/passwd -p war -k passwd_watch
5. sudo ausearch -k passwd_watch
6. Discuss how regular audit logging might have prevented or reduced breach impact.

**Reflection Questions (2 points):**

- What would you include in a cloud incident response plan?
- Why is logging critical in breach detection?