III.) Network infrastructure:

- •) owner: IT Department
- •) Role: connectivity, communication, & data transfer
- •) Risks:
  - Network breaches
  - Data interception
  - Downtime & disruptions
- •) mitigation strategies:
  - Firewalls & intrusion detection.
  - secure protocols (HTTPS, SSH)
  - Regular network monitoring & updates.

IV) Software: Algorithms:

- •) owner: Research Team/developers.
- •) Role: Data analysis, simulation, & modelling
- •) Risks:
  - intellectual property theft
  - Licensing breaches
  - Error or biases
- •) mitigation strategies:
  - Licensing agreements & contracts.
  - secure code repositories.
  - Peer reviews & testing.

ASSET IN COMPUTER DEPARTMENT LAB

Shaurya Srivastava,
23370059
ISM ASSIGNMENT

I) Computer System

- Owner : IT Department
- Role : Data analysis , research & communication
- Risks : Cybersecurity threats , data breaches, or system failure
- Mitigation strategies : Regular updates, antivirus software , firewalls , access controls , & data backups

II) Sensitive Research Data

•) Owner : Researcher team

•) Role : Data collection , analysis & storage

•) Risks : Data loss or theft.
- Unauthorised access
- compliance breaches.

•) Mitigation : - Regular maintenance & ~~calt~~ calibration
- Secure storage & access control.
- training & safety protocols.

V) Confidential Documents:

*) owner: Faculty /staff

*) Role : Research, administrative & personnel records.

*) Risks:

- unauthorized access.
- Data breaches
- compliance breaches.

*) mitigation strategies:

- Secure storage & shredding
- Access controls & authentication
- Encryption & digital signatures.

VI) Servers:

*) owner: System Administrator

*) Role: Hosting applications, data storage, & backups.

*) Risks: Downtime, data breaches.

*) mitigation: Implementing redundancy, regular security updates & monitoring.

VII Cabling & connectivity Equipments

*) owner : Network Technician

*) Role: connecting devices to the network

•) Risks: Poor organization leading to hazards, connection failures.

•) mitigation: Proper cable management & regular inspections.

VIII) Security systems (e.g firewalls, antivirus)

•) owner: Security officer

•) Role: Protecting systems from threats.

•) Risks: cyberattacks, malware infections

•) mitigation: Regular updates, Employee training on Security practices, & monitoring.

ix) Power supply units:

*) owner: Lab technician

*) Role: providing backup power during outages

*) Risks: Failure during power loss.

*) mitigation : Regular testing & maintenance.

X) Printers & scanners

*) owner: IT Department

*) Role : Printing & scanning services

*) Risks: Data theft, unauthorized access

*) mitigation strategies: secure print jobs, restrict access.

XI) Password management systems:

·) owner: IT Department

·) Role: Secure password storage

·) Risks: Password compromise, unauthorized access..

·) mitigation strategies: Implement multi-factor authentication, regular password updates.

XII) Routers & switches

*) owner: IT Department

*) Risk : Network breach, downtime

*) Role: manage network connectivity.

*) mitigation : Regular firmware updates secure configuration.

XIII) Productivity software (Eg. microsoft office)

- owner: IT Department
- Risk: Licensing breaches, data theft
- Role: Support productivity & document creation
- mitigation: License management, access controls.

XIV Lab schedules & calendars:

- owner: Lab administrators
- Risk: Data loss, scheduling conflicts.
- Role: manage lab resources & scheduling
- mitigation: Regular backups, access controls.

XV Lab Access & Security Protocols:

- owner: Lab administrator
- Risk: unauthorized access, security breaches
- Role: Ensure secure access to lab resources

mitigation: Regular reviews, updates.