NAME AND ENROLLMENT NUMBER	DEPARTMENT
Lukhi Laksh - SR25MSAD016	MSC AI/DS

	DESCRIPTION
CRITICAL DATA	Data that can be tampered by any means.
VULNERABLE DEVICES	Devices that can be accessed by unauthorized entity.

TASK-1

TYPE	DEVICE	NUMBER OF DEVICES
CAL ASSET INVENTORY	LAPTOPS	3
	MOBILE PHONES	5
	TABLETS	2
	EXTERNAL HARDRIVES(HDD AND SSD)	4
	CCTV CAMERS	3
	USB THUMB DRIVES	2
	ROUTERS	2
	MODEM	1
	WIRELESS ACCESS POINTS	1
DIGITAL ASSET INVENTORY	GMAIL	3
	GOOGLE DRIVE	3
	ICLOUD	2
	BANKING	2
LIST OF ALL THE PERSONNEL WORKING IN THE COMPANY INCLUDING THE OWNER	OWNER	1
	MANAGER	1
	STAFF	3

LOCATION	TYPE OF WORK PLACE
SURAT	SHOWROOM
SURAT	WAREHOUSE
SURAT	BACKOFFICE

TASK-2

MULTI-FACTOR AUTHENTICATION(MFA)	-
LEAST PRIVILEGES	WE NEED TO ENSURE THAT ONLY THE OWNER HAS THE PRIVILEGE TO ACCESS THE DATA COMPLETELY AND ALL THE OTHER STAFF INCLUDING THE MANAGER CAN ONLY ACCESS THE DATA ACCORDING TO THE ROLES THEY ARE ASSIGNED.
CREDENTIAL SECURITY	WE NEED TO USE A SAFE AND BUSINESS GRADE PASSWORD MANAGER TO STORE ALL THE PASSWORDS FOR MANAGER AND OWNER
ENCRYPTION OF DATA	EVERY EXTERNAL HARDDRIVE , SSD AND USB THUMBDRIVE HAS TO BE ENCRYPTED SO THAT IF THEY ARE LOST THE DATA IS NOT MISUSED AND
HARDENING NETWORK HARDWARE OR SECURITY	CHANGE THE DEFUALT ADMIN PASSWORD ON THE MODEM AND WAP . AND WE NEED TO ENSURE THAT WIFI USES WPA3 ENCRYPTION IF
AUTO-UPDATES	SET ALL DEVICES TO AUTO-UPDATE SO THEY CAN PATCH WITH THE LATEST UPDATES AND SECURITY MEASURES EASILY AND AUTOATICALLY
PHISHING SIMULATION	-
PHYSICAL SECURITY	-

TASK-3

This Incident Response Simulation uses a "Tabletop Exercise" format. We will simulate a high-probability th mobile phone belonging to a staff member in the Surat Showroom, which has access to your critical Goo

STEPS THAT WE WILL FOLLOW

STEP	GOAL	ACTION
DETECT	Identifying that an incident is occurring.	The staff member immediately reports the loss to the Manager.

RESPOND(PHASE-1 CONTAINMENT)	Stop the "bleeding" and prevent the thief from accessing the "Red/Critical" data.	1.Remote Wipe: The Owner or Manager uses the MDM (Protect Strategy) to send a "Kill Signal" to the phone, erasing all data remotely.
		2.Account Lockout: Log into the master Google Admin console and "Sign Out" all sessions for that staff member's account.
		3.Bank Alert: Call the bank to temporarily freeze mobile banking access for that specific device ID.
RESPOND(PHASE-2 ERADICATION AND ANALYSIS)	Understand what happened and remove the threat	1.Check Logs: Check the Google Drive "Activity" log. Did any files get downloaded or shared in the 20 minutes between the theft and the remote wipe?
		2.Credential Reset: Change the passwords for any apps that were on that phone, even if you think the phone was locked.
RECOVER	Restore the staff member's ability to work and ensure no data was lost.	1.Device Replacement: Issue a new device and immediately apply your PROTECT strategy (Encryption + MFA) before it enters the showroom.
		2.Data Verification: Confirm that the Personnel List on Google Drive is intact and hasn't been tampered with.
GOVERN & IMPROVE (Post-Incident Activity)	Learn from the mistake so it doesn't happen again.	1.The "Post-Mortem": Why was the phone on the counter and not in a secure locker?
		2.Policy Update: Create a new rule: "No personal or business mobile devices are to be left in public-facing showroom areas."

DESCRIPTION

reat based on your inventory: a stolen gle Drive and Banking information.

SIMULATION QUESTION
Does your staff know exactly who to call the second they realize the phone is gone? If they wait until the end of their shift, the "Window of Vulnerability" grows.

-		
-		
-		