**SME Security Blueprint Design**

**1. Project Scope**

* **SME Description:**
  + Type of business: Small Manufacturing company
  + Number of employees: 25
  + Location(s):West Midlands
* **Key Assets:**
  + Physical: office space, equipment, inventory, vehicles (vans)
  + Digital: designs, customer data, financial data, internal communications

**2. Risk Assessment**

* **Identified Threats:**
  + Physical: robbery, theft (equipment),fire, accidents and natural disasters
  + Cyber: data breaches, malware infections, phishing and ransomware
* **Vulnerabilities: malware infections, outdate software, weak passwords**
* **Potential Impacts: financial loss, identity loss and reputational damage**

**3. Physical Security Measures**

* **Office Layout Design:**
  + Surveillance areas: separated areas where the front of the shop (Showroom) is for the public and the workshop in the back (restricted area) is separated to protect the public
  + Access control points: shop front door
  + Safe zones: shop front (Showroom) and the fire evacuation location
* **Physical Barriers and Systems:**
  + Type of barriers: heavy doors which require a keycard for access to separate the showroom from the workshop
  + Security systems (alarms, cameras): CCTV, fire alarms, physical security guard
  + Access control mechanisms: authorised workers are given a keycard to access in the back, workers are required to wear PPE when working such as eye protection, safety shoes and helmets, , finished toys on display are locked in a cabinet for display only
  + **Visitor and Employee Access Policies:**   
    A sign is put up of rules to follow for customer safety, employees can only access the workshop when they are in uniform, all visitors must have their visitor’s ID with them at all times, All visitors must wear helmets ,a fire escape plan is put up in the shop for the safety of both staff, visitors and customers

**4. Cybersecurity Policies**

* **Password Management:**
  + Requirements: all passwords should be 8 characters or longers with a combination of numbers and special characters, should not include any personal information such as last names or D.O.B
  + Change frequency: every 6 months
* **User Roles and Access Levels: Minimal only given the amount of access that would be needed to complete that task**
  + Provisioning process: implement
  + Deprovisioning process: Implement principle of least privelige, implement the separation of duties

**5. Monitoring and Response Plans**

* **Monitoring Systems:**
  + Physical security: CCTV and alarms, physical patrols and have employees report any suspicious behaviours
  + Cyber security: install IDS & IPS, Install Anti virus and Anti malware software, utilise SIEM Tools to monitor security logs
* **Incident Response Plan:**
  + Physical breach: create a simple to understand and documented emergency security plan for physical breaches such as a fire or a robbery
  + Cyber breach: create different response plans for different cyber breaches (phishing, malware, estc), have a point of contact to coordinate people during a security breach
* **Communication Plan: create a documented plan of how to alert relevant stakeholders when a security incident has occurred**

**6. Education and Training**

* **Security Awareness Training:**
  + Topics: Phishing, social engineering, Malware, safe browsing practices and general computer security and safety, Fire and robbery
  + Frequency: every 6 months
* **Drills and Exercises:**
  + Types: Fire, robbery, phishing and social engineering attacks
  + Schedule: Every 3 months

**7. Maintenance and Review**

* **Review Schedule: Every 6 months**
* **Maintenance Routines: Every 3 months** 
  + Physical security systems: Ensure that all CCTV and alarms are up to date and test if they work without any issues
  + Cybersecurity systems: Ensure that all systems receive the latest updates and patches, conduct Penetration tests, conduct simulated phishing tests on employees to check their security awareness

**8. Documentation**

* **Blueprint Document:**
  + Sections included:   
    physical and digital assets   
    physical and digital security measures   
    cyber policies  
    incident response plan  
    education and training  
    maintenance schedule
* **Appendices:**
  + Quick-reference guides:
  + Emergency contacts:   
    Head of IT  
    important stakeholders
  + Glossary of terms:  
    IDS = Intrusion Detection system   
    IPS = Intrusion prevention system   
    Firewall = responsible for filtering anything that leaves or enter a network Stakeholders = someone who has interest in the activities of a business

**9. Presentation**

* **Summary of Key Points:   
  Create strong passwords  
  Create strong physical security measures**Create strong cyber Security measures
* Ensure we are well educated on cyber attacks and safe browsing techniques
* **Intended Audience:   
  All employees and management**
* **Presentation Medium:Hotel conference room**

**10. Reflection**

* **Challenges Faced:   
  Weak cyber security measures,   
  out of date systems   
  non existent security measures for systems  
  weak network security**
* **Solutions and Overcomings:   
  -create stronger passwords,   
  -update and patch systems as well as purchase new equipment to replace the old ones  
   install a firewall  
  install new anti virus and anti malware software**
* **Areas for Improvement😐  
  incident response plan  
  incident detection   
  Network security**
* **Future Enhancements:  
  -Update all the security systems both physical and cyber  
  -Audits every 6 months   
  -risk assesments and vulnerability scans every 3 months   
  -Install SIEM tool to ensure that the security logs can be monitored  
  -Provide all employees and management with the relevant cyber security safety training and sage browsing techniques   
  -Penetration tests every 3 months   
  -Phishing and social engineering simulations every 3 months to see -if the employees recognise a cyber attack, to see how they react to cyber attacks and see what they would do in that situation**