Solution

Security Policies:

- **Password Policy:**
  - Update password policy
  - Use minimum 12 characters
  - Combination of upper and lowercase
  - Incorporate letters, numbers and special symbols
  - Must not be simple
  - Changed every 90 days

- **Backup and recovery policy:**
  - 3-2-1 backup strategy for the maximum protection
  - Incorporate on-premise and cloud solutions
  - Use of external harddrives and cloud backups of important files and data
  - Implementation of incremental backups
- **Access Controls:**
  - Implement RBAC
  - Provide minimum access needed to do the job
  - Regular auditing of the access control policy to ensure there is no escalation of privileges being given to an unauthorized user

Infrastructure:

- **Updated equipment:**
  - Sam's Scoops should invest in new computers to so that they are up to date and manufacture provides the support for those products
  - Automatic updates should be enforced so that as soon as the new updates are available for the system, the device installs it in order to reduce the chances of a vulnerability to get exploited by the threat actor
- **Firewall Configuration:**
  - Sam's Scoops should hire a IT consultant or cybersecurity analyst to configure the firewall
  - Firewall configuration is required to filter the incoming and outgoing traffic
  - Sam's Scoops should use the firewall to block the ports that they wont need and can be used by cybercriminals to Sam's Scoops' network such as Port 80
- **Authentication Protocols:**
  - Sam's Scoops should enforce use of MFA
  - All the employees should have to verify their identity two ways before having access to the system

    - Sam’s Scoops can incorporate applications such as Microsoft Authentiactor, Google Authenticator and Authy to address the authentication needs

Physical Safety:

- **Physical safety:**
    - All the devices that are used by Sam’s Scoops should be out of the reach of unauthorized personal
    - Network devices such as Modem, Routers and Switches should be adequately secured and should not be placed in a location where anyone can have access to them
    - A secure control room can be used to house these devices
    - Area accessed by employees for conducting business operations such as entering orders, accepting financial payments should not be accessible to the customers or any outsiders
    - If needed, a security guard can be hired to protect these physical locations from unauthorized access
- **Remote access:**
    - Sam’s Scoop should use appropriate and secure protocols for remote access
    - Use of VPN services should be incorporated for a secure and protected remote access