Assignment: In this project, you'll create a security infrastructure design document for a fictional organization. The security services and tools you describe in the document must be able to meet the needs of the organization. Your work will be evaluated according to how well you meet the organization's requirements.

About the organization: This fictional organization has a small, but growing, employee base, with 50 employees in one small office. The company is an online retailer of the world's finest artisanal, hand-crafted widgets. They've hired you on as a security consultant to help bring their operations into better shape.

Organization requirements: As the security consultant, the company needs you to add security measures to the following systems:

- An external website permitting users to browse and purchase widgets
- An internal intranet website for employees to use
- Secure remote access for engineering employees
- Reasonable, basic firewall rules
- Wireless coverage in the office
- Reasonably secure configurations for laptops

Since this is a retail company that will be handling customer payment data, the organization would like to be extra cautious about privacy. They don't want customer information falling into the hands of an attacker due to malware infections or lost devices.

Engineers will require access to internal websites, along with remote, command line access to their workstations.

Grading: This is a required assignment for the module.

What you'll do: You'll create a security infrastructure design document for a fictional organization. Your plan needs to meet the organization's requirements, and the following elements should be incorporated into your plan:

- Authentication system
- External website security
- Internal website security
- Remote access solution
- Firewall and basic rules recommendations

- Wireless security
- VLAN configuration recommendations
- Laptop security configuration
- Application policy recommendations
- Security and privacy policy recommendations
- Intrusion detection or prevention for systems containing customer data

Security Infrastructure Design Document (SIDD):

Purpose:

The purpose of this document is to define the security infrastructure design for a retail company's information systems. This design ensures that all digital assets, including customers data, internal applications, and network resources, are protected from unauthorized access, misuse, and potential compromise. It provides a structured blueprint for implementing, maintaining, and improving security controls across on-premises and remote access.

The document supports the company's mission to deliver reliable and confidential retail services while ensuring compliance with local data protection regulations and international standards such as ISO/IEC 27001, NIST SP 800-53, and PCI DSS.

Security Measures to the Organization Requirements:

1: An external website permitting users to browse and purchase widgets:

• Maintain the CIA triad, confidentiality, integrity, and availability of customer data which helps ensure strong defense mechanisms against attacks such as Distributed Denial-of-Service (DDoS) attacks.

• Implement the AAA authentication, authorization, and accounting.

- **Authentication:** Is this user who they claim to be?
- **Authorization:** What is this user allowed to do?
- **Accounting:** What did this user do?

• Create complex and lengthy passwords containing numbers, special characters, Upper and lowercase characters.

• Install digital certificates (issued by a trusted Certificate Authority) on a server so that secure communication can happen — and both the server and clients can trust and authenticate each other.

• Defined and well-established privacy policies are an essential part of acceptable privacy practices. Set guidelines on customer data handling in place.

• Assessing website for vulnerabilities.

2: An internal intranet website for employees to use:

• Continuously monitor network traffic and intranet activity to identify unusual behavior. Implement an **Intrusion Detection and Prevention System (IDS/IPS)** to detect and automatically block suspicious activity or unauthorized access attempts targeting the intranet.

• Use simple but secure login through employee credentials. Apply role-based access (e.g., managers, sales staff, admin) and enable two-factor authentication (2FA) for users who handle sensitive data.

• Host the intranet on a local company server or secure cloud service that is accessible only from within the company's private network. Use a firewall to block unauthorized access and set up a VPN for remote connections if needed.

• Protect all communication with HTTPS (TLS certificates) even for internal use. Encrypt important business information such as employee records and sales summaries stored in the database.

• Keep the server operating system, intranet software, and antivirus tools up to date. Limit administrative rights to a few trusted employees, and disable default or unused accounts.

• Enable basic logging to track user logins, changes, and access attempts. Regularly review logs for unusual activity, even if automated SIEM tools are not in place.

• Follow secure development practices—validate user input, avoid default passwords, and test the intranet for vulnerabilities before deployment. Use regular backups before making software updates.

• Schedule automatic backups of intranet data (daily or weekly) to an external hard drive or secure cloud storage. Test data restoration occasionally to ensure recovery in case of system failure.

• Conduct short security awareness sessions for employees—teach them about safe password use, phishing risks, and proper intranet behavior. Establish a simple acceptable use policy that all employees must follow.

3: Secure remote access for engineering employees:

• Deploy a Virtual Private Network (VPN) (e.g., OpenVPN or WireGuard) to allow engineers to securely connect to the company's internal network and intranet. Ensure the VPN uses strong encryption (AES-256) and requires authentication before access.

• Integrate multi-factor authentication (MFA) for all remote logins. Use role-based access control (RBAC) so engineers only access systems or repositories relevant to their work, such as development servers or code repositories.

• Require all devices used for remote access to have updated antivirus software, firewall enabled, and automatic system updates. Consider using endpoint management tools (like Microsoft Intune or MDM) to enforce security settings

• Enforce HTTPS, SSH, and SFTP for all data transfers between remote devices and company servers. Prohibit insecure protocols (e.g., FTP, Telnet).

• Enable connection and activity logs on VPN and remote servers. Regularly review logs for suspicious behavior, such as repeated failed logins or unusual connection times.

• Ensure that critical project files and engineering data are stored on centralized, backed-up servers, not personal laptops. Use encrypted backups and restrict data download permissions when possible.

• Train staff on remote work security best practices, including device security, recognizing phishing attempts, and using VPNs properly. Establish a Remote Access Policy defining acceptable use, password rules, and reporting procedures for security incidents.

4: Reasonable, basic firewall rules:

• Block all incoming traffic by default and only allow approved services — such as HTTPS (port 443) for the company website, VPN access for remote employees, and specific ports for internal systems that need remote management.

• Permit employee devices and servers to connect only to essential business services (e.g., web browsing, email, DNS, software updates). Block unnecessary outbound connections to prevent malware or data exfiltration.

• Place the company website and any online services behind a Web Application Firewall (WAF) to filter malicious requests (like SQL injection or DDoS attacks) while still allowing customers normal web access over HTTPS.

• Separate internal business systems (e.g., HR data, POS systems, and intranet) from public-facing servers and guest Wi-Fi. Apply firewall rules between segments to control access and reduce internal risks.

• Record all firewall activity (especially denied connections) and review logs regularly. Set up alerts for suspicious behavior, repeated failed connection attempts, or abnormal traffic patterns.

5: Wireless coverage in the office:

• Ensure strong and consistent Wi-Fi signal across all work areas — including employee desks, meeting rooms, and storage areas — with no dead zones or weak spots.

• Create separate wireless networks for different purposes — for example, one for employees, one for guests or customers, and one for critical business systems (like POS terminals or internal servers).

• Protect all Wi-Fi networks with WPA3 encryption (or at least WPA2) and strong passwords. Limit access to the internal network to authorized devices only through MAC filtering or authentication systems.

• Use multiple access points (APs) strategically placed to handle 50 users comfortably without congestion. Choose dual-band (2.4 GHz and 5 GHz) APs for better performance and reliability.

• Periodically check wireless performance, coverage, and interference. Update firmware, adjust channel settings, and monitor for unauthorized access points (rogue APs).

6: Reasonably secure configurations for laptops:

• Require unique employee accounts with strong passwords and multi-factor authentication (MFA) for logging in and accessing sensitive company systems. Disable shared or guest accounts.

• Enable full disk encryption (e.g., BitLocker for Windows or FileVault for macOS) to protect company data if a laptop is lost or stolen.

• Configure laptops to automatically install operating system and security updates, including browser and antivirus patches, to minimize vulnerabilities.

- Install reputable antivirus/endpoint security software, enable the built-in device firewall, and restrict installation of unauthorized applications.

- Store business data on secure company servers or cloud storage, not on local drives. Set user permissions to limit access based on job roles, and ensure regular encrypted backups are performed.