Security Infrastructure Design Document

1. Authentication System:
   - Implement a Multi-Factor Authentication (MFA) system for user authentication on all systems to enhance security.
   - Enable strong password policies, including regular password changes and complexity requirements.

2. External Website Security:
   - Use SSL/TLS encryption to secure communication between users and the website.
   - Implement Web Application Firewall (WAF) to protect against common web vulnerabilities like SQL injection and cross-site scripting.
   - Regularly scan the website for vulnerabilities and apply security patches promptly.

3. Internal Website Security:
   - Use access control lists to restrict access to sensitive internal resources based on user roles.
   - Implement network segmentation to isolate internal systems from external threats.
   - Conduct regular security training for employees to prevent social engineering attacks.

4. Remote Access Solution:
   - Set up a Virtual Private Network (VPN) for secure remote access to internal resources.
   - Utilize two-factor authentication for remote access to enhance security.
   - Ensure all remote endpoints are encrypted and have updated security software.

5. Firewall and Basic Rules Recommendations:
   - Configure the firewall to block unnecessary ports and services.
   - Create access control policies to allow only authorized traffic.
   - Regularly review firewall logs for suspicious activity.

6. Wireless Security:
   - Enable WPA2 or WPA3 encryption on the wireless network to prevent unauthorized access.
   - Implement a hidden SSID to make the network less visible to potential attackers.
   - Regularly update firmware for wireless access points to address known vulnerabilities.

7. VLAN Configuration Recommendations:
   - Implement VLANs to segregate network traffic and enhance security.
   - Use VLAN tagging to control access and prevent unauthorized connections between different network segments.
   - Implement VLAN access control lists to restrict communication between VLANs.

8. Laptop Security Configuration:
   - Encrypt all laptops to protect data in case of theft or loss.
   - Install endpoint security solutions, including antivirus and anti-malware software.
   - Enable laptop tracking and remote wipe capabilities to secure devices remotely.

9. Application Policy Recommendations:
- Enforce application whitelisting to prevent unauthorized software installations.
- Regularly update and patch all applications to address vulnerabilities.
- Implement least privilege access to limit application permissions.

10. Security and Privacy Policy Recommendations:
- Develop and enforce a comprehensive security policy outlining acceptable use guidelines and security best practices.
- Implement data privacy controls to protect customer information and comply with relevant regulations.
- Regularly review and update security and privacy policies to adapt to changing threats and compliance requirements.

11. Intrusion Detection or Prevention for Systems Containing Customer Data:
- Deploy Intrusion Detection Systems (IDS) to monitor network traffic for suspicious activity.
- Implement data loss prevention (DLP) solutions to prevent unauthorized access or exfiltration of customer data.
- Regularly audit and review security controls to ensure the protection of customer data.