For this company we will need to implement AAA. Authentication can be done by asking the user for their user id and password, OTP or biometrics. Authentication means verifying the user who they claim they are and to grant them access by matching the credentials when they are prompted to enter them with the credentials on the authentication server. The server would then authorise the user and grant them access. External website security will be required to prevent hackers from attempting security breaches. etc.) Firewalls can be used internally at different stages and the website should also be placed in a DMZ providing limited access to internal resources. Firewalls should have ACLs configured which would prevent requests to unsafe websites to enter through the company's defence in depth layers. Firewalls can be configured with rules to allow only specific kind of traffic (prevention of DDoS) Proxies should be configured in order to hide the origin of requests to external websites. The website should also be signed by a CA to and configured to work with HTTPS. A SIEM tool can be configured to monitor the company's infrastructure from one place and use alerts to detect suspicious activity. Policies should be implemented on user's devices limiting permissions and forcing strict controls such as password strength. An internal website should be limited to users internally using access control and users should be educated on how to use the website. VPNs can be used to provide remote access to engineering users. To enable a user for remote access and manage their access to protect assets, we can use remote desktop protocols and managing server sessions. We should also Implement tools and techniques for backup and disaster recovery. Wireless access security should also be implemented to restrict access to Wi-Fi to prevent malicious activities. Wireless security can be provided by the use of encryption, decryption, authentication and authorization. VLANs are an importation part of a company's infrastructure which allows logical dividing of a network. VLANs can be configured between router and firewall, router and gateway, router and switch and by doing so one can filter the web traffic that passes the network.

Using a password with a combination of OTP or Biometrics, VPN and registering the laptop by their MAC address will provide laptop security. Endpoint security tools should also be running on user laptops which allow for monitoring.

Application policy includes use of cookies, social media integration, access control and generating notifications as per organization and IT rules.

Security policies should be implemented for traffic filtering, IP spoofing, user authentication and other specific policy for the website. Most Endpoint protection tools come with IPS/IDS capabilities. IPS is implemented behind the firewall and it matches the incoming traffic against the security policies. It matches the signature and handles the intrusion if any and generates the log and alerts for the same. IDS goal is to identify malicious traffic before it can proceed further into the network. It generates alerts and notification so that the network monitoring team can look after the intrusion. Use of anomaly-based detection with IPS would be the ideal choice.