**Web Hosting Security Proposal**

To ensure that the newly designed website is securely hosted, it's important to consider several key factors that will protect both the site and its users. While the current website does not store sensitive information, it is essential to plan for future scalability, ensuring security features can handle future expansions and protect any sensitive data that may be introduced.

**1. Secure Hosting Environment**

The first step is to choose a reliable hosting provider that offers built-in security features. Key hosting security features to look for include:

* **SSL Certificate**: Encrypts data transferred between the website and users, protecting sensitive information.
* **Firewalls**: Protect the hosting environment from unauthorized access and cyber-attacks.
* **Backup and Recovery**: Regular backups ensure that data is not lost during an attack and can be quickly recovered.
* **Server Monitoring**: Real-time monitoring of the hosting server can help detect and prevent potential breaches.

**2. Access Control and User Management**

Implementing strong access controls is crucial for limiting administrative access to the website. Multi-factor authentication (MFA) and role-based access control (RBAC) will help ensure that only authorized personnel can modify critical website components. Regular audits of user accounts should also be conducted to ensure no unauthorized access.

**3. Content Management System (CMS) Security**

If a CMS (e.g., WordPress) is used, it’s vital to apply security patches and updates as soon as they are released. Keeping plugins and themes up to date minimizes vulnerabilities. Additionally, limit the number of plugins to only those necessary to reduce the potential attack surface.

**4. Data Encryption**

Although the website currently does not handle sensitive data, it is recommended to encrypt any personal or financial data that could be stored or processed in the future. End-to-end encryption ensures that even if data is intercepted, it cannot be read by unauthorized parties.

**5. Regular Security Audits and Penetration Testing**

Conducting regular security audits and penetration testing will help identify vulnerabilities and fix them before they can be exploited. This proactive approach ensures continuous protection and adaptability to emerging threats.

**Conclusion**

Securing the hosting environment is critical for protecting the website's integrity and future expansions. By implementing the above strategies, we can ensure that the website remains safe from cyber threats while providing a secure platform for future growth.