NexSoft Software Development Plan

GOALS

1. Strong security controls for sensitive data and cloud resources.
2. Meet industry standards for data protection and compliance.
3. Ensure smooth user experience while enforcing strict access controls.

Development Phases

1. **Requirements Gathering**
    1) Collect detailed security needs to protect sensitive data.
    2) Focus on role-based access control, data encryption, and anti-phishing measures.
    3) Outline requirements to ensure compliance with industry standards.

2. **Architecture Design**
    1) Design a layered security model for strong data protection.
    2) Set up a zero-trust model where all access requires verification.
    3) Plan for end-to-end encryption to secure data in transit and storage.

3. **Threat Modeling**
    1) Conduct a comprehensive threat analysis on data handling and access points.
    2) Prioritize threats like phishing, insider misuse, and cloud vulnerabilities.
    3) Regularly review threat models to keep up with evolving risks.

4. **Implementation**
    1) Set up RBAC to limit access based on user roles.
    2) Integrate anti-phishing tools and train users to recognize phishing attempts.
    3) Use data encryption to protect information stored in the cloud and during transfers.

5. **Testing**
    1) Run security tests to check the effectiveness of access controls and phishing defenses.
    2) Conduct misuse testing to spot vulnerabilities from insider threats.
    3) Perform compliance audits to verify adherence to industry standards.

6. **Deployment**
    1) Use a secure deployment pipeline with built-in security checks for updates.
    2) Confirm RBAC is enforced consistently in all deployed environments.
    3) Install anti-malware tools across systems to guard against ransomware attacks.

7. **Post-Deployment Maintenance**
    1) Regularly scan for vulnerabilities and apply necessary patches.
    2) Monitor for unusual activity, especially among users with high access levels.
    3) Implement a response plan for phishing, insider threats, and malware attacks.