Security

TYPO3's Built-In Security

Purpose: Ensure robust protection of user data and safeguard government websites against security threats

Secure Authentication & Role-Based Access Control	TYPO3 provides secure login mechanisms, support for multi-factor authentication (with proper configuration), and fine-grained permission settings for backend users.
Input Validation and Sanitization	TYPO3 has built-in routines to sanitize and validate user input, reducing the risk of SQL injection, XSS, and other common vulnerabilities.
Session Management	Secure session handling is integrated into TYPO3, with options to configure secure cookies (using Secure and HttpOnly flags) and session timeouts.
Data Protection & Encryption	The system supports HTTPS enforcement and must be configured to encrypt sensitive data, aligning with best practices for data security.
Logging and Monitoring	TYPO3 includes logging capabilities that capture security-related events, aiding in monitoring and incident investigation.
SSL Certificate	Obtain SSL certificates from reputable and trusted Certificate Authorities (CAs) to ensure credibility and widespread browser compatibility. Monitor the expiration dates of SSL certificates and set up automated reminders or renewals to prevent service disruptions. Ensure that TYPO3 installations enforce HTTPS across all pages.
Additional Considerations	Ensure proper configuration verifying that TYPO3's security settings are correctly configured to meet your specific government website requirements. Consider adding custom measures such as regular security audits and penetration testing. Keep up with TYPO3 security advisories, updates and best practices

Security for Other Applications (Web-based and Mobile)

While TYPO3 provides a strong security foundation, additional web-based and mobile applications require dedicated security measures. The following guidelines ensure consistent, high-level security practices across all platforms.

Secure Coding Practices	Implement secure coding standards to prevent vulnerabilities. Perform static code analysis and regular code reviews to identify and resolve security issues.
API Security	Protect API endpoints with robust authentication, encryption, and rate limiting. Use token-based authentication (e.g., OAuth) and ensure sensitive data is never exposed.
Third-Party Integrations	Keep all third-party components updated and monitor for any security advisories.
Access Control & Identity Management	Implement role-based access control (RBAC) to limit user permissions and minimize risk.
Data Protection & Encryption	Ensure all data transmitted between applications, whether web-based or mobile, is encrypted using TLS/SSL. Apply encryption to sensitive data stored in databases or transmitted through APIs.
Regular Security Audits	Conduct regular vulnerability assessments and penetration testing across all platforms. Maintain an incident response plan that covers both web and mobile environments.
Monitoring & Incident Response	Set up centralized logging and monitoring tools to detect and respond to potential security breaches. Integrate with a SIEM (Security Information and Event Management) system to analyze security events in real time.