**MESD Documentation LMS-95-Security**

**Purpose**

To allow for high level of security in the system and safe guarding user information.

**Background**

The MESD LMS will be hosted and housed by the 1Gov 1Citizen platform. This initiative exists to provide services to provide residents of Botswana in a more efficient and effective manner. The MESD LMS will need to be secured.

**How it’s done?**

Security is a critical aspect of any LMS, and Moodle incorporates various security measures to protect user data and ensure a secure learning environment. Here's an exhaustive list of security measures employed in Moodle:

1. **User Authentication:**
   * Username and password authentication.
   * Support for multi-factor authentication (MFA).
   * Integration with external authentication systems (LDAP, OAuth, Shibboleth, etc.).
2. **Data Encryption:**
   * Transport Layer Security (TLS) encryption for data in transit.
   * Encryption of sensitive data such as passwords and personal information.
3. **Access Control:**
   * Role-based access control to determine user privileges.
   * Fine-grained permissions allowing administrators to control access to specific features and resources.
4. **Secure Password Policies:**
   * Password complexity requirements.
   * Password expiration and history to enforce regular updates.
5. **Account Lockout Policies:**
   * Configurable account lockout after multiple failed login attempts.
   * Automatic unlocking after a specified period.
6. **Session Management:**
   * Session timeout settings.
   * Secure session handling to prevent session hijacking.
7. **Security Headers:**
   * Implementation of HTTP security headers (Content Security Policy, Strict-Transport-Security, etc.) to enhance browser security.
8. **Cross-Site Scripting (XSS) Protection:**
   * Code and content filtering to prevent malicious script injection.
9. **Cross-Site Request Forgery (CSRF) Protection:**
   * Use of anti-CSRF tokens to validate and authenticate user requests.
10. **SQL Injection Prevention:**
    * Parameterized queries and input validation to prevent SQL injection attacks.
11. **File Upload Security:**
    * Restrictions on file types and sizes for uploaded materials.
    * Scanning uploaded files for malware.
12. **Logging and Auditing:**
    * Comprehensive logging of user activities and system events.
    * Regular review and analysis of logs for security monitoring.
13. **Security Updates and Patch Management:**
    * Timely application of security patches and updates.
    * Regular system vulnerability assessments.
14. **Firewall Protection:**
    * Network-level firewalls to control incoming and outgoing traffic.
15. **Data Backups:**
    * Regular backups of critical data to prevent data loss in case of a security incident.
16. **Incident Response Plan:**
    * A documented plan for responding to security incidents.
    * Training and awareness programs for users and administrators.
17. **External Integrations Security:**
    * Secure integration protocols.
    * Regular security assessments of third-party plugins and integrations.
18. **Security Awareness Training:**
    * Training for users and administrators on security best practices.
    * Information dissemination regarding current security threats.
19. **Vulnerability Scanning and Penetration Testing:**
    * Regular security assessments to identify and address vulnerabilities.
    * Periodic penetration testing to simulate real-world attacks.
20. **GDPR Compliance:**
    * Measures to ensure compliance with data protection regulations.
    * User consent and data privacy controls.
21. **Community Collaboration:**
    * Active participation in the Moodle community to stay informed about security best practices.
    * Prompt communication and collaboration on security issues.