PURPOSE

This LMS Manual provides guidance for the secure, efficient, and compliant delivery of distance learning, e-learning, and blended learning courses at SEATECH. It ensures proper use of the platform, protects learner data, and supports consistent learning outcomes while complying with MARINA Circular NO. SC-2021-10 and the Data Privacy Act of 2012.

SCOPE

This manual applies to all SDLS users, including trainees, instructors, assessors, and concerned personnels. It covers:

1. User registration, authentication, and access management.
2. Security, data privacy, and system compliance.
3. Delivery infrastructure, multimedia content, and communication tools.
4. Supported operating systems, browsers, and applications.
5. Assessment and interactive learning activities.
6. Backup, maintenance, and incident reporting.
7. Instructor guidance for course management, monitoring, and feedback.

DEFINITION OF TERMS

Learning Management System (LMS) – online platform used by SEATECH to deliver, manage, and monitor distance learning, e-learning, and blended learning courses. The LMS is named *Seatech Distance Learning System (SDLS).*

Authentication – process by which a user verifies their identity to access the SDLS, including password validation and optional two-factor authentication.

Privilege / Role-Based Access – system permissions assigned to users based on their designated role, controlling access to SDLS functions and data.

Self-Assessment – activities or exercises within the SDLS where trainees reflect on their learning and evaluate their own progress.

Video and Sound Formats – digital media specifications supported by the SDLS to ensure proper delivery of multimedia course content.

Terms and Conditions – binding rules and policies governing SDLS usage, including confidentiality, system security, data privacy, and compliance requirements.

Receiving Technology – devices, operating systems, browsers, and applications used by trainees to access SDLS content and activities.

Delivery Infrastructure – technical and administrative systems enabling the distribution of course materials, communication, and interaction between trainees, instructors, and administrators.

Access Control – process of restricting and managing user access to the SDLS based on assigned roles and permissions to ensure data security and system integrity.

Account Deactivation – process of disabling a user's access to the SDLS due to course completion, withdrawal, inactivity, or policy violation.

Audit Log – system-generated record that tracks user activities within the SDLS, including login attempts, access history, and system changes for monitoring and compliance purposes.

Backup System –process of creating copies of SDLS data at regular intervals to ensure recovery in case of data loss, system failure, or security incidents.

Data Protection Officer (DPO) – The designated individual responsible for ensuring compliance with data privacy laws and handling data protection concerns.

De-registration – The formal removal or termination of a user's access to the SDLS.

A. SECURITY AND INTELLECTUAL PROPERTY

1. E-LEARNING SYSTEM SECURED FROM TAMPERING AND ATTEMPTS TO HACK INTO THE SYSTEM

1. Registration, User Access Management and Authentication

Registration

a. All trainees shall be duly registered in the Seatech Distance Learning System (SDLS), with complete documentary requirements submitted and the required enrollment payment settled prior to confirmation of enrollment.

b. Upon successful registration and enrollment confirmation, trainees shall be enrolled in the Seatech Distance Learning System (SDLS) prior to accessing any course materials, learning activities, or assessments. Each trainee shall be assigned a unique username using the Seafarer's Registration Number (SRN) and a system-generated temporary password. Login credentials shall be sent to the trainee's registered email address.

c. Upon first login, trainees shall be required to immediately change the system-generated temporary password to ensure account confidentiality, security, and prevention of unauthorized access.

d. The IT Officer shall create the corresponding course, batch, and training schedule in the SDLS and enroll all officially registered trainees in the appropriate course assignment.

e. Once officially enrolled in the system, trainees shall only be granted access to the specific course, modules, learning materials, and assessments in which they are officially registered.

User Access Management

a. Role-based access control shall be implemented to ensure that users can only access SDLS functions and data relevant to their assigned role.

b. Access privileges are defined as follows:

- *Trainees* – Access limited to enrolled courses, training materials, learning activities, assignments, formative assessments, and summative assessments. Authorized to participate in teaching-learning activities and submit all required course outputs and assessment responses through the SDLS.

- *Instructors / Assessors* – Access to course content, trainee attendance and progress, assessment management, grading, validation, and activity logs. Authorized to admit or remove trainees during synchronous sessions.

- *Registrar* – Responsible for creating accounts of confirmed enrollees and assigning courses and batches in the SDLS.

- *Research and Development Department (RDD)* – Authorized to create and update course content, including asynchronous materials, assessments, interactive activities, and related instructional components.

- *MARINA STCW Office* – Provided with a dedicated inspection account for monitoring, surveillance, and compliance verification purposes. Access credentials shall be readily available as required.

- *Invigilator* – Authorized to monitor examinations, supervise assessment sessions, and review activity logs during scheduled assessments.

- *IT / System Administrator* – Full SDLS management and monitoring privileges, including system configuration, user management, security settings, and audit log access. Create, suspend and terminate an existing user's access rights for a specified period of time or indefinitely.

c. Access rights shall be reviewed periodically to ensure continued compliance with MARINA requirements and SEATECH policies.

d. Accounts shall be suspended or revoked immediately upon:

- Course completion or official withdrawal (for trainees)
- Resignation or termination of employment (for staff)
- Violation of SDLS policies or security protocols

Authentication and Security Controls

In compliance with MARINA requirements, the SDLS shall implement the following authentication and security measures:

a. The SDLS shall implement a flexible and secure privilege-based access control system that enables host-based verification.
b. User access levels are assigned based on role and system permissions.
c. All login activities are recorded for audit and monitoring purposes.
d. All password traffic transmitted between user devices and the SDLS server shall be encrypted.
e. Passwords are stored in encrypted format within the system database to prevent unauthorized access.
f. Login system is protected by re-CAPTCHA verification to prevent automated access attempts and unauthorized system intrusion.
g. The SDLS shall implement Two-Factor Authentication (2FA) using any of the following:
    - Username and password; or
    - Time-based One-Time Pin (OTP) sent via registered email.

    Note: Two-factor authentication shall be required for administrators and may be enabled for other user roles as part of enhanced security controls.
h. The system shall provide a secure “Forgot Password” function for all users.
i. Password reset requests shall be verified through the user’s registered email address.

Protection Against Brute Force Attacks

The SDLS shall implement the following security controls:

- Accounts with three (3) consecutive failed login attempts shall be automatically blocked.
- Password recovery may be facilitated by the assigned Administrator through the administration panel, subject to identity verification.
- Users shall be automatically logged out after 4 hours of inactivity. Idle timeout settings may be configured by the IT Officer.
- Only alphanumeric characters shall be allowed in the username and password fields.
- Accounts that remain inactive for 395 days shall be temporarily disabled and subject to review.
- The system shall provide a password reset tool accessible to end users through a verified email request process.
- All login attempts, password resets, account lockouts, and authentication activities shall be logged and retained by the system.

Back-Up System Intervals or Auto Back-Up System

The SDLS is equipped with an automatic backup feature. To ensure data integrity and continuity, all SDLS data, including but not limited to course content, student records, assessment results, and certificates, is backed up every Sunday.

- All backups are securely stored cloud storage to prevent data loss.
- Only authorized SDLS Administrators have access to backup files.
- Backups are retained for at least 90 days to allow recovery of historical data if needed.
- The IT/ System Administrator shall ensure that backups are completed successfully.
- The system maintains previous versions of critical data to allow restoration to a specific point in time if necessary.

Reporting Procedures in the Event of Breaches

SEATECH establishes a structured procedure to ensure the **timely detection, reporting, assessment, containment, and resolution** of any data breaches, unauthorized access, or suspicious activity within the Seatech Distance Learning System (SDLS).

a. Any detected breach, unauthorized access, or suspicious activity must be reported immediately to the Data Protection Officer (DPO) and the IT Department.
b. Upon detection, the incident shall be formally documented using the SDLS Incident / Data Breach Reporting Form (NAGA-ITD-QPF10-00-26)
c. If the SDLS is accessed outside authorized hours or by an unauthorized account, the system shall automatically lock the affected account to prevent further unauthorized activity.
d. A complete incident report shall be prepared, including the following minimum details:

- Incident details
- Incident severity level
- Systems and data affected
- Root cause / source of breach
- Corrective and preventive actions
- Recovery actions (if applicable)
- Current status of the incident

e. The DPO or IT/System Administrator shall conduct an initial assessment to determine:

- Nature and severity of the breach
- Systems and data affected
- Possible operational impact
- Potential regulatory implications

f. Audit logs shall be retrieved and analyzed to identify the source, timeline, and activity related to the breach.

g. The incident shall be further evaluated to determine its operational and regulatory impact, including potential exposure of sensitive data and system disruption.
h. Appropriate notifications shall be issued to the following, as applicable:
   - Affected users
   - Concerned departments and authorized personnel
   - Regulatory authorities, if required (e.g., Maritime Industry Authority (MARINA) or National Privacy Commission (NPC))
i. The breach shall be immediately contained to prevent further damage. Containment measures may include:
   - Password resets
   - Revocation of access privileges
   - Account suspension or lockout
   - System isolation
j. The IT Officer shall implement recovery actions, including:
   - Application of system patches or configuration fixes
   - Restoration of data from the latest verified backup (if necessary)
   - System recovery and validation
k. After containment and recovery, the IT Department shall:
   - Recommend security enhancements
   - Strengthen system controls
   - Address identified vulnerabilities
   - Implement preventive measures to reduce recurrence
l. All actions taken—from detection, reporting, assessment, containment, recovery, and closure—shall be:
   - Fully documented in the official incident report
   - Stored securely for audit and compliance purposes
   - Made available for internal and external review when required

Routine Updates or Maintenance Schedules of the SDLS Platform

SEATECH ensures the reliability, security, and availability of the Seatech Distance Learning System (SDLS) through a structured routine update and maintenance schedule. The SDLS undergoes regular software updates to address security patches, bug fixes, system improvements, and feature enhancements.

a. The IT / System Administrator conducts monthly maintenance, or as required, based on system needs and security advisories.
b. Maintenance activities are performed manually by the IT Officer and are scheduled during **non-training hours** to avoid disruption of scheduled classes and assessments.
c. The maintenance schedule is submitted to the DL Supervisor and Training Director for approval prior to implementation using SDLS Routine Updates & Maintenance Schedule (NAGA-ITD-QPF-07-00-26)
d. A maintenance notice is sent to users via email at least 24 hours in advance. The notice includes:
   - Date and time of maintenance

- Expected downtime duration
- Scope of work
- Any temporary workarounds for ongoing training activities

e. A final reminder is posted one (1) hour before the maintenance window.
f. During the scheduled maintenance period, the SDLS website becomes temporarily inaccessible to prevent system conflicts and ensure data integrity.
g. The SDLS is placed in maintenance mode prior to system updates to prevent data loss.
h. Upon completion, maintenance mode is disabled and full system access is restored.
i. The IT Officer verifies that all updates and patches were successfully applied.
j. SDLS performance is monitored for 24– 48 hours post-maintenance to detect any unexpected errors or slowdowns.
k. Any user-reported issues shall be addressed immediately by the IT/ System Administrator.
l. All maintenance activities, communications are properly documented and securely stored.

Server and Firewall Configurations

The Seatech Distance Learning System (SDLS) operates within a secure cloud-based server environment protected by properly configured firewall and network security controls.

a. The SDLS is hosted on a secured cloud server with access limited to authorized IT personnel. Administrative access requires strong authentication credentials.
b. Firewalls and cloud security tools monitor and control incoming and outgoing traffic. Only necessary ports and services for SDLS operations are enabled, while unauthorized access attempts are blocked.
c. Secure communication protocols (HTTPS) encrypt all data transmission between users and the SDLS.
d. Server and firewall logs are regularly monitored to detect suspicious activities. Any unusual access attempts are investigated immediately.

Secure Against Unauthorized Access or Accidental Loss

SEATECH implements appropriate technical and administrative safeguards to protect the Seatech Distance Learning System (SDLS) against unauthorized access, misuse, alteration, disclosure, or accidental loss of data.

a. User access is role-based and limited to authorized personnel only.
b. Unique usernames and strong passwords are required for all users.
c. Accounts are automatically locked after repeated failed login attempts.
d. Secure HTTPS encryption is enforced for all SDLS transactions.
e. Sensitive information is stored securely within the system database.
f. Monthly backups are performed and securely stored to prevent data loss.
g. Suspicious activities are immediately investigated by the IT Officer.
h. The SDLS automatically logs out inactive users after 8 hours.
i. Any unauthorized access or data breach is reported and managed in accordance with established Incident report procedure.

j. A legitimate user unintentionally deletes courses, questionnaires, or trainee submissions, the IT shall restore files in back-ups.
k. In case of accidental data loss, the SDLS can restore information from secure weekly backups.

NOTE: Please refer to ***1.1. Registration, User Access Management, and Authentication*** for the complete details on SDLS security.

Policies with Information of Review at Planned Intervals - Information Security

The Seatech Distance Learning System (SDLS) information security controls are reviewed annually or as required to maintain effectiveness, ensure compliance, and identify vulnerabilities.

1. The IT/System Administrator schedules the SDLS Information Security Review and notifies all concerned personnel.

2. Relevant information is gathered, including:
   - User access logs and permissions
   - Backup and recovery status
   - System logs for unusual or suspicious activity
   - MARINA circulars and advisories related to SDLS or Distance Learning (DL)
   - Any previous security incidents and corrective actions

3. A review agenda is prepared, highlighting areas to assess, including compliance, system security, and performance.

4. Review Meeting - The IT/System Administrator, concerned departments, and Top Management convene to:
   - Verify compliance with MARINA circulars and relevant regulations
   - Assess system performance and security controls
   - Evaluate effectiveness of backups and incident responses
   - Identify vulnerabilities or potential improvements

5. Minutes of the review, findings, and action plans are recorded and submitted to Top Management for approval.

6. The IT/System Administrator implements the agreed actions within assigned timelines. Progress is monitored for 60 days, and any deviations shall be addressed promptly.

7. All changes resulting from the review are communicated to the concerned departments for information.

8. All review documentation, including minutes shall be maintained.

Terms and Conditions

The Seatech Distance Learning System (SDLS) shall display clearly defined Terms and Conditions that govern its use, with an emphasis on the protection of confidential and sensitive information. These Terms and Conditions shall be legally enforceable and accessible to all users upon registration and prior to accessing SDLS resources.

1. All users must read and accept the SDLS Terms and Conditions before being granted access.
2. The Terms explicitly require users to maintain the confidentiality of all sensitive data, including training records, assessment results, and any personally identifiable information.
3. The Terms are drafted in accordance with applicable laws and regulations, making violations legally actionable.
4. The Terms and Conditions are prominently displayed on the SDLS login or registration page and are accessible at any time through the user interface.
5. Acceptance of the Terms is logged, and non-compliance or breaches shall be subject to investigation and corrective actions.
6. Any changes to the Terms and Conditions shall be communicated to all users, and acceptance of the updated Terms is required before continued access to the SDLS.
7. A mandatory click-through “I Agree” consent banner shall be deployed upon first login.

Terms and Conditions

By accessing this SDLS and clicking or checking “I Agree,” you confirm that you have read, understood, and agree to comply with all Terms and Conditions stated below.

These Terms are designed to protect system integrity, ensure confidentiality, and comply with applicable laws and regulations.

1. Acceptance of Terms

Access is granted only to authorized users who have read and accepted these Terms. Logging into the SDLS constitutes acknowledgment and agreement to comply with all rules, policies, and procedures governing system use.

2. User Responsibility and Account Security

Users are responsible for maintaining the confidentiality of their login credentials. Account sharing is prohibited. Any activity performed under a user’s account shall be the responsibility of the registered account holder.

3. Protection of Confidential Information

All SDLS content, including training materials, assessments, records, and system data, is confidential and proprietary. Users shall not copy, distribute, or disclose any content without proper authorization.

4. Compliance with Data Privacy Laws

Personal data collected in the SDLS (such as names, training records, assessment results, ID details, and similar information) shall be used solely for legitimate training, certification, and administrative purposes, in accordance with the Data Privacy Act of 2012 (RA 10173). Users consent to such data processing.

5. Monitoring, Recording, and Proper Use

Users acknowledge and consent that SDLS activities, including training sessions, assessments, and system access, may be monitored or recorded through logs, screen capture, webcam, or audio/video recording to ensure assessment integrity, training verification, and regulatory compliance.

Users must use the SDLS solely for authorized training and educational purposes. Any attempt to bypass system controls, manipulate assessments, access restricted data, introduce malicious software, or disrupt system operations is strictly prohibited.

6. Assessment Integrity

During SDLS-based assessments, users must follow all rules and instructions. Cheating, impersonation, unauthorized assistance, or system manipulation may result in invalidated results, restricted access, or other disciplinary actions.

7. System Security

Any suspected unauthorized access, security vulnerability, or misuse must be immediately reported to the system administrator. SEATECH may investigate and take appropriate actions to maintain system security.

8. Modification of Terms

SEATECH may update these Terms due to regulatory changes, system improvements, or operational requirements. Users shall be informed of any updates, and continued use of the SDLS constitutes acceptance of the revised Terms.

9. Termination or Suspension of Access

SEATECH reserves the right to suspend, restrict, or terminate SDLS access without prior notice for violations of these Terms, unauthorized activities, system security breaches, academic dishonesty, or misuse of confidential information. Additional administrative actions may be taken in accordance with institutional policies and applicable regulations.

By clicking “I Agree,” you acknowledge that you have read, understood, and accept all responsibilities, rules, and policies described above, including monitoring, recording, data privacy compliance, and possible disciplinary measures.

SECURE AGAINST UNAUTHORIZED ACCESS OR ACCIDENTAL LOSS

1. User Registration and De-Registration Procedure

. User Registration

User registration in the Seatech Distance Learning System is controlled and managed by authorized personnel to ensure that only legitimate and authorized users are granted access.

1. Registration of Trainees

For trainees, the registration process is managed by the Registrar.

- The trainee completes the onsite or online enrollment process for the selected training course.
- Upon confirmation of enrollment and payment**,** the Registrar creates a user account in the SDLS.
- Each trainee is assigned a unique username and a temporary password.
- The trainee is granted access only to the specific course or training program in which they are officially enrolled.
- The login credentials are sent to the trainee through the registered email address.
- Upon first login, the trainee is required to change the temporary password and acknowledge the SDLS Terms and Conditions.

2. Registration of Other Users

For system users such as MARINA Personnels, Instructors, Assessors, RDD personnel, and other authorized staff, account creation and access management are handled by the IT/System Administrator**.**

- The requestor submits an access request using User Registration-Other Authorized Users Form (NAGA-ITD-QPF-08-00-26)
- Once the request is approved, the IT/System Administrator creates the user account in the SDLS based on the approved request.
- Each user is assigned a unique username and a secure password.
- Access privileges and system permissions are assigned according to the user's designated role and responsibilities within the SDLS.

b. User De-Registration

User de-registration ensures that access to the SDLS is removed immediately when it is no longer required, preventing unauthorized use of the system.

- When a trainee withdraws his/her enrollment, the trainee shall accomplish an Amendment Form. Upon approval, the Registrar shall initiate the account deactivation process.
- If a user account is suspected of unauthorized use, compromise, or violation of SDLS policies, the Registrar or IT Officer shall temporarily suspend or deactivate the account pending investigation.
- For instructors, administrators, assessors, RDD personnel, or other system users, the IT/System Administrator shall deactivate the account upon request or when access is no longer required.

- De-registered accounts are immediately disabled, and all access to SDLS resources and services is revoked.

0. Privilege Management

Privilege management ensures that access to information and system functions is restricted, controlled, and monitored according to user roles and responsibilities.

. Every SDLS user, including learners, instructors, assessors, system administrators, and technical staff, is assigned a unique username.
. Usernames are linked to the individual to ensure accountability for all system activities.
. Access privileges and permissions are assigned based on the user's role and responsibilities. ***(User Access Management)***
. Users may only access data and perform functions necessary for their role.
. Privileges are granted, modified, or revoked only by authorized personnel (Registrar for trainees, IT/System Administrator for other users).
. Users cannot grant privileges to themselves or other users.
. When a user's role or job function changes, the Department Head shall submits a privilege modification request using the IT Platform Account Creation and Modification Request Form (NAGA-ITD-QPF-09-00-26).

0. User Password Management

User password management ensures that passwords are securely allocated, managed, and monitored to protect access to the SDLS.

a. System auto-creates a user with a random character password, where the trainee is required to change the temporary password upon first log in.
b. Password allocation, reallocation, and recovery are controlled through a formal management process:
- Registrar – trainees
- IT/System Administrator – Instructors, assessors, and other users

c. Password recovery is performed only by the assigned administrator using the SDLS administration panel.
d. All password changes, resets, and failed login attempts are logged for monitoring and audit purposes.
e. Users must agree and acknowledge Terms and Conditions confirming that they will keep their password confidential.

4. Password User Guide

To ensure secure use of passwords, users must follow these guidelines:

a. Must be unique to the SDLS and not reused from other systems.
b. Only alphanumeric characters are allowed; the system may allow additional special characters if supported.
c. Minimum complexity requirements:
- At least 8 characters
- Combination of uppercase and lowercase letters

- Inclusion of numbers

d. Avoid easily guessable information such as name and birthdate.
e. Temporary passwords must be changed immediately upon first login.
f. User passwords must kept confidential, do not share or write them down in unsecured locations.
g. Idle sessions of 4 hours will automatically log out the user.
h. Accounts inactive for 395 days will be temporarily disabled.
i. The system has password reset tool to be managed by the end user requested via email.

5. Registration Support

A registration support mechanism is established to assist users who encounter difficulties accessing the SDLS, including password recovery, login failures, or other account-related concerns.

1. Users who have forgotten their password may click the “Forgot Password” available on the SDLS login page.
2. The system will prompt the user to enter their registered email address associated with their SDLS account.
3. Upon submission, the SDLS will automatically send a Password Reset Link to the registered email address.
4. The user must open the email, click the reset link, and follow the on-screen instructions to create a new secure password in accordance with the Password User Guide.
5. This password reset process is designed as a self-service mechanism, requiring no intervention from the IT/System Administrator unless technical issues arise.
6. To enhance system security, the SDLS utilizes Google CAPTCHA during login attempts to ensure that the request is made by a legitimate human user and not an automated system.
7. The system lock accounts after 3 failed login attempt to protect the system from unauthorized access.
8. If a user is confident that their login credentials are correct but still cannot access the SDLS, the user must contact the designated SDLS Technical Support through the official support email or contact number for assistance.
9. IT/System Administrator shall verify the identity of the user before providing assistance and may coordinate with the Registrar or concerned personnel to investigate and resolve the issue when necessary.

6. Session Time-out

To protect user accounts and sensitive data from unauthorized access resulting from idle or unattended sessions, the Platform shall implement an automatic session timeout mechanism.

- Accounts that remain idle for 4 hours shall be automatically logged out. This idle time may be configured by the IT Officer in accordance with operational requirements.
- Accounts that remain inactive for 395 days shall be temporarily disabled until reactivated by the System Administrator.
- Upon logout or temporary disablement, users must re-enter their credentials to regain access.
- Any unsaved data during idle periods may be lost; users are strongly encouraged to save their work regularly.
- Users are responsible for logging out manually when leaving their device unattended and for protecting their account credentials.

0. Review of User Access Rights

1. The IT/System Administrator, DL Supervisor, Registrar, and other concerned personnel shall conduct reviews of all SDLS user accounts semi-annually or as required to ensure permissions align with current roles and responsibilities.
2. The IT/System Administrator shall generate a complete list of SDLS users, including their assigned roles and permissions.
3. Each user's assigned access shall be verified against their current job function, enrollment status, or operational requirements.
4. Any user with excessive, outdated, or inappropriate permissions shall be flagged for adjustment.
5. All modifications to access rights must be approved by the DL Supervisor prior to implementation.
6. Access for users no longer affiliated with SEATECH shall be removed immediately.
7. Privileged accounts shall be restricted to authorized personnel only.
8. All changes in access rights, including revocations and modifications, shall be logged with timestamps, approvers, and reasons to maintain an auditable record.
9. Users whose access is revoked or modified shall be notified promptly.

8. Data Privacy Act Compliance

The SDLS shall comply with R.A. 10173 otherwise known as the "Data Privacy Act of 2012", in order to respect and protect the privacy of each individual/applicant as prescribed in the abovementioned law.

1. The system shall comply with the Data Privacy Policy, as approved by the institution's Data Privacy Officer, and shall fully adhere to the requirements of the Data Privacy Act of 2012 as enforced by the National Privacy Commission.
2. The Data Privacy Statement shall be posted in the Front-End System and shall notify the users every time they log in.
3. No personally identifiable information may be exposed within and outside the system without proper authorization as privacy of the user data shall be dealt with utmost priority.
4. Any attempt to breach the security will be recorded with all the relevant data.

5. If the system is accessed in the time not defined by the System Administrator, e.g., in the case of production deployment, all options will be locked and the user will not be able to use the system.
6. Reports can be retrieved for all audit logs.

B. TRAINEE IS ABLE TO SYSTEMATICALLY REFLECT LEARNING THROUGH SELF-ASSESSMENT AND INSTRUCTOR AND INSTRUCTOR-MARKED ASSIGNMENTS

The SDLS shall provide opportunities for trainees to systematically reflect on their learning through self-assessments, instructor-marked assignments, and interactive course activities. Digital documents and course tools shall facilitate learner engagement and reflection, including but not limited to:

1. *Assignments*
   - Tasks designed to assess knowledge, skills, and application of course content.

0. *Discussion Forums*
   - Structured online discussions where trainees can share insights, ask questions, and collaborate with peers and instructors.

0. *Feedback*
   - Constructive feedback from instructors on assignments, quizzes, and forum participation to guide learning progress.

0. *Interactive Content / Engagement*
   - Multimedia elements, quizzes, simulations, and other interactive tools to actively engage learners with the course material.

0. *Reading Material Reflections*
   - Guided exercises prompting trainees to reflect on and summarize key concepts from course readings.

- The SDLS shall display visual indicators to monitor trainee participation. A *red status indicator* shall appear for activities or assignments that have not yet been completed by the trainee, while a *green status indicator* shall appear once the trainee has completed or submitted the required activity.

- Instructors shall review and mark all submitted assignments and activities within the SDLS. The system shall allow instructors to monitor the status of each trainee's submission, including whether the assignment is pending, submitted, reviewed, or graded, to ensure proper tracking of learner progress.

C. USERS MANUAL FOR INSTRUCTORS

Instructor's Manual for Utilization and Navigation of the SDLS

The Seatech Distance Learning System (SDLS) shall include a dedicated *Instructor's Manual* that provides comprehensive guidance on the proper utilization and navigation of the platform. This manual shall be accessible only to authorized instructors and shall remain *hidden from students* to preserve the integrity of assessment and course management.

The Instructor's Manual shall contain clear instructions on the following:

1. Procedures for logging into the SDLS and accessing instructor dashboards.
2. Navigation of the SDLS interface, including course management tools and system features available to instructors.
3. Procedures for creating and managing assignments, quizzes, formative assessments and other activities within the system.
4. Guidelines for reviewing submissions, grading assignments, and providing feedback to trainees.
5. Monitoring trainee participation, progress, and completion status.
6. Utilization of communication tools such as discussion forums, announcements, and messaging features.
7. Procedures for maintaining assessment integrity, including proper marking of assignments and monitoring of trainee engagement.
8. Troubleshooting basic system issues and reporting technical concerns to the SDLS System Administrator.

Delivery Infrastructure

The training course delivered through distance, e-learning, or blended learning modes shall be supported by a reliable and fast internet connection or other suitable fixed connection to ensure uninterrupted access.

1. A mechanism shall be in place to allow trainees to:
   - Receive all course materials in a timely and appropriate sequence.
   - Access the course instructor and fellow participants for discussions and queries.
2. This access can be facilitated by any of the following means:
   - Disk/downloaded data
   - Internet connection (while in port or via fixed connection)
   - An appropriate blend of the two proceeding means
3. SEATECH shall document and utilize existing communication tools to enable seamless interaction for trainees. These include, but are not limited to:
   - Telephone
   - Email
   - Learning platforms
   - Virtual classrooms (accessible via the SDLS only)

Receiving Technology

1. **Operating Systems**
   - The SDLS supports all operating systems officially maintained and supported by their respective manufacturers.
   - The system is designed to remain compatible with a wide range of operating systems, including both current and earlier supported versions, to ensure accessibility for trainees using different devices.
   - A compatibility evaluation mechanism tests and verifies whether new operating system versions support the SDLS and current course content.
   - A recommended list of operating systems is provided to trainees prior to enrollment to guide optimal system setup.
   - The SDLS functions properly across all supported operating systems and web browsers, including Google Chrome, Microsoft Edge, and Mozilla Firefox.
   - Trainees are informed in advance of the recommended operating systems, browsers, and any required applications or plugins.
   - Clear instructions for installation, setup, and troubleshooting of all required technology are included in the SDLS Manual.
   - Mechanisms ensure that trainees using older operating systems or alternative browsers can access all course content without limitations.

Video and Sound

- The SDLS supports all current and acceptable older video and sound formats to ensure full access to multimedia course content.
- Trainees are notified in advance if there are changes to recommended video or sound versions.
- A compatibility mechanism tests and verifies that new video and sound formats function correctly with the SDLS and current course content.
- Recommended video and sound formats, including suggested versions, are provided to trainees prior to enrollment.
- Documentation, including descriptions, instructions, and screenshots or photos, is included in the SDLS Manual to demonstrate compatibility.
- Access is ensured for trainees using older systems, and records are maintained to verify proper functionality.

Internet Browsers

- The SDLS platform supports all current and acceptable older web browsers to ensure full access to course content across existing operating systems.
- Trainees are notified in advance if there are any changes to supported browser versions.
- A compatibility mechanism tests and verifies that new browsers function correctly with the SDLS and current course content, and a recommended list of browsers is provided to trainees.
- An automatic system check is available for trainees to verify their system and receive recommendations for necessary browser upgrades.