REGIONAL MEMORANDUM
No. 1412, s. 2025

STRENGTHENING SECURITY MEASURES FOR DIGITAL SYSTEMS

To : **All Schools Division Superintendents**
All Others Concerned

1. This is in reference to the Memorandum No. OASIC-MEM-101425-T3-1 dated October 14, 2025, titled Strengthening Security Measures for Digital Systems.

2. The increasing number of security incidents targeting Department of Education (DepEd) digital platforms, all ICT concerned personnel, system and website administrators in all field offices are directed to conduct regular and thorough security assessments. This is to ensure that all DepEd-managed systems and websites are properly configured, secured and protected against all forms of potential threats.

3. The recommended security measures and other additional provisions are detailed in the attached Memorandum.

4. For queries and/or concerns, you may contact Mr. Sean Michael Brucal of the ICTS-TID through email at icts.tid@deped.gov.ph or via landline at 02-8633-2363.

5. For information, guidance and strict compliance.

TOLENTINO G. AQUINO
Director IV

Reference: None
Encl.: None
To be indicated in the Perpetual Index
under the following subjects:

ICT SYSTEMS/WEBSITES

ORD/ICTU/SCL/RM_SucurityMeasureDigitalSystems
October 16, 2025

Republic of the Philippines
Department of Education
OFFICE OF THE ASSISTANT SECRETARY
INFORMATION AND COMMUNICATIONS TECHNOLOGY

MEMORANDUM
OASICT-MEM-101425-T3-1

TO : **REGIONAL AND DIVISION IT OFFICERS**
ALL OTHERS CONCERNED

FROM : **ATTY. MARCELINO G. VELOSO III**
Assistant Secretary

SUBJECT : **STRENGTHENING SECURITY MEASURES FOR DIGITAL SYSTEMS**

DATE : 14 October 2025

1. In light of the increasing number of security incidents targeting Department of Education (DepEd) digital platforms, all Information Technology (IT) Officers, system administrators, and website managers are hereby directed to conduct regular and thorough security assessments to ensure that all systems and websites are properly configured, secured, and protected against potential threats.

2. All concerned are further instructed to immediately disseminate and implement this directive among ICT personnel and other staff involved in the administration and maintenance of DepEd-managed systems and websites.

3. **Recommended Security Measures**

3.1. *Asset Inventory and Classification.*

3.1.1. Maintain an updated inventory of all digital assets, including servers, domains, systems, endpoints, and databases.

3.1.2. Classify data (e.g., public, internal, confidential) and apply security measures appropriate to each classification level.

3.1.3. Assign accountability for each system or platform (system owner, administrator, custodian).

3.2. *Network Security and Segmentation.*

3.2.1. Apply network segmentation to separate public-facing systems from internal administrative systems.

3.2.2. Use VPNs or secure tunnels for remote administrative access.

3.2.3. Enable rate-limiting, DDoS protection, and WAF (Web Application Firewall) for publicly accessible sites.

3.3. *Conduct Comprehensive Security Scans.*

3.3.1. Perform regular vulnerability and malware scans on all DepEd-managed systems, websites, and servers.

3.3.2. Ensure that antivirus, firewall, and intrusion detection systems are properly configured and continuously updated.

3.4. *Review Folder and File Permissions.*

3.4.1. Verify that directory and file permissions follow the principle of least privilege.

3.4.2. Restrict access to sensitive folders and ensure public directories are set to read-only where applicable.

3.5. *Secure Upload Folders and Modules.*

3.5.1. Configure upload modules or directories to accept only approved file types (e.g., .pdf, .jpg, .png).

3.5.2. Disallow executable or script files (e.g., .php, .js, .asp, .exe, .sh) to prevent malicious uploads or defacement.

3.5.3. Implement server-side file validation and sanitization for all uploads.

3.6. *Apply System and Software Updates.*

3.6.1. Regularly install the latest security patches and updates for operating systems, CMS platforms, and web applications.

3.6.2. Remove or disable unused plugins, modules, or accounts that could expose vulnerabilities.

3.7. *Monitor for Unauthorized Activities.*

3.7.1. Routinely inspect system logs and website directories for unauthorized changes or suspicious uploads.

3.7.2. Maintain secure, verified, and up-to-date backups of all critical systems and data.

3.8. *Strengthen Authentication and Access Controls.*

3.8.1. Enforce strong password policies and enable multi-factor authentication (MFA) for all administrative accounts.

3.8.2. Periodically review user privileges and ensure that access is limited to authorized personnel only.

3.9. *Reporting and Coordination.*

3.9.1. Immediately report any detected vulnerabilities, suspicious activities, or potential breaches to the Division or Regional ICT Unit for proper action and coordination.

3.9.2. Copy furnish all reports to cert@deped.gov.ph.

4. All ICT personnel are required to implement the above measures and maintain the highest level of vigilance in protecting DepEd's digital platforms, systems, and data.

5. While comprehensive capacity-building initiatives are forthcoming, the above measures must be strictly observed in the interim to ensure continued protection of DepEd's ICT infrastructure.

6. This Office is currently undertaking a comprehensive review and update of existing ICT security policies, standards, and operational guidelines. This initiative includes the development of updated training, certification, and upskilling programs to strengthen the cybersecurity capabilities of all ICT personnel at the regional, division, and school levels.

7. These measures aim to ensure that recognized industry best practices are institutionalized across all DepEd offices and digital platforms. The updated policies and capacity-building activities will be rolled out in the coming months, with specific implementation timelines and compliance requirements to be issued through subsequent advisories.

8. For guidance and strict compliance.

9. For further clarification on this matter, please contact Sean Michael Brucal of the Information and Communications Technology Service-Technology Infrastructure Division at (+632) 8633-2363 or via email at icts.tid@deped.gov.ph.