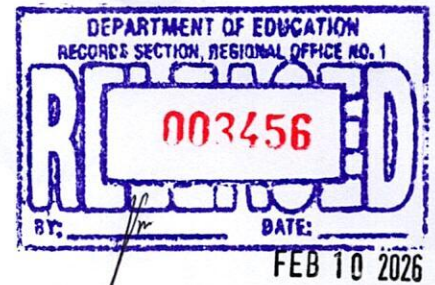




Republic of the Philippines
Department of Education
REGION I



OFFICE MEMORANDUM

No. 45, s. 2026

**IMPLEMENTATION OF DEPED RO1 PERSONNEL SECURITY MEASURES
FOR DIGITAL SYSTEMS AND PLATFORMS**

To: Assistant Regional Director
Chief of the Functional Division
Section/Unit Heads
All Concerned Personnel

1. Due to the increasing number of security incidents targeting Department of Education (DepEd) digital platforms, all ICT-concerned personnel, system and website administrators are hereby directed to conduct regular and thorough security assessments. This ensures that all DepEd-managed systems and website are properly configured, secured and protected against all forms of potential threats.

2. In addition, the recommended security measures for DepEd personnel when using digital platforms are as follows:

a. Account and Password Security

- Use strong password (at least 12 characters, using a mix letters, numbers symbols).
- Enable Multi-Factor Authentication (MFA) on all DepEd issued accounts (Google, Microsoft, Adobe Suite, Canva, etc.).
- Do not share passwords with anyone.
- Change passwords regularly and avoid reusing passwords across other platforms.
- Use the official DepEd email for work-related digital activities.

b. Device Protection

- Keep laptops, tablets and mobile devices updated with the latest security patches.
- Install only authorized and trusted applications.
- Enable device screen locks and auto-lock timers.
- Use antivirus software and ensure it stays updated.
- Avoid using public computers to access DepEd systems.



Republic of the Philippines
Department of Education
REGION I

c. Secure Internet and Network Usage.

- Connect only to trusted and secured Wi-Fi networks.
- Avoid accessing DepEd platforms using public Wi-Fi without VPN.
- Never share DepEd network credentials (e.g. Wi-Fi passwords).

d. Data Protection and Privacy Compliance

- Follow DepEd's Data Privacy policies when handling student, teachers and administrative data.
- Store sensitive information only in authorized platforms (e.g. DepEd Microsoft OneDrive).
- Do not use personal accounts (Gmail, Facebook, personal drives) to store official documents.
- Encrypt or password protected sensitive files before sharing.

e. Email and Communication Safety

- Be cautious with emails asking for login details or personal information – these are often phishing attempts.
- Check sender details before opening attachments.
- Report suspected phishing emails to the ICT unit.
- Avoid clicking unfamiliar or suspicious links.

f. File Sharing and Cloud Storage

- Share files only through:
 - DepEd email
 - DepEd OneDrive
 - Official DepEd-approved platforms
- Set proper sharing permission (e.g. "view only" or "specific people")
- Avoid uploading sensitive data to non-DPED platforms.

g. Social Media Conduct

- Keep professional boundaries when communicating with students, DepEd personnel and stakeholders.
- Do not post sensitive information on social media.
- Avoid oversharing screenshots of:
 - Official documents
 - Chats
 - Internal systems
 - Students and DepEd personnel



Republic of the Philippines
Department of Education
REGION I

h. Continuous Cybersecurity Awareness

- Participate in ICT training, webinars and orientation.
- Stay updated on new DepEd advisories regarding:
 - Email security
 - Cyber threats
 - Data privacy guidelines

i. Incident Reporting and Response

- Immediately report in the ICT Unit:
 - Suspected hacking or unauthorized access
 - Lost of stolen devices
 - Data breaches
 - Malware infections
- Document the incident and inform the ICT Unit as required.

3. For information, guidance and strict compliance.

TOLENTINO G. AQUINO
Director IV

ORD-ICTU/scl/OM_SecMeasureDigiPlatforms
February 5, 2026



DepEd RO1



Documan 8

ICTU260009