Republic of the Philippines
Department of Education
National Capital Region
SCHOOLS DIVISION OFFICE
CITY OF MUNTINLUPA

July 25 , 2017

DIVISION MEMORANDUM
No. 109, s. 2017

DepEd - MUNTINLUPA
RELEASED
DATE 7/27/17

To: **OIC – Asst. Schools Division Superintendent**
Chief, CID and SGOD
Division Supervisor /District Supervisors/Coordinators
Elementary and High School Principals/Officers-In-Charge
Division Personnel Officer
Division and School Information Technology Officer
All Concern

SECURITY OF ENTERPRISE HUMAN RESOURCE INFORMATION SYSTEM (eHRIS)

1. Attached is the Memorandum from the Office of the Director, Aida C. Yuvienco Director IV Information and Communication Technology Service dated July 21, 2017 **RE: Security of Enterprise Human Resource Information System (eHRIS)**, contents of which are self-explanatory, for the information and guidance of all concerned.

2. Immediate dissemination of this Memorandum earnestly is desired.

MAURO C. DE GULAN, Ed. D.
Schools Division Superintendent

Republic of the Philippines
Department of Education
INFORMATION AND COMMUNICATIONS TECHNOLOGY SERVICE
Pasig City, Philippines

Office of the Director

MEMORANDUM

TO: Regional Directors
Schools Division Superintendents and Officers-in-Charge
Public Elementary, Junior and Senior High School Heads and Officers-In-Charge
Region and Division Personnel Officers
Region and Division Information Technology Officers
All concerned

FROM: **AIDA C. YUVIENCO**
Director IV

SUBJECT: **Security of Enterprise Human Resource Information System (eHRIS)**

DATE: 21 July 2017

We acknowledge the growing concern regarding the security of eHRIS. We are issuing this memo to allay the fears of employees regarding this issue.

The concern emanated from Caloocan Public Elementary and Secondary Teachers Federation (CPESTF) that was posted in their Facebook Page highlighting a message "not secure" that appeared in the browser's address bar while accessing the site. This occur when the site does not have an SSL certificate.

Please be assured that we are in the process of implementing HTTPS in ALL our web applications. While this is ongoing, we have put in place other mechanisms to secure our data and applications and these are:

- Web encryption of critical data such as passwords.
- Host servers are protected by an enterprise firewall both software and hardware.
- We have a facility to monitor malicious attempts to penetrate our network.

However, research show that 70% of breaches in information security result from human error. Information security is a concern and responsibility of everyone, so we enjoin you to observe the following precautions:

- Refrain from using public computers and wi-fi.
- If above cannot be avoided, ensure that you close the browser and logoff.
- DO NOT SHARE YOUR PASSWORD.
- Do not leave your computer open. If you need to take a break, logoff from the application and lock your computer.
- Ensure that your Operating System (OS) is updated.
- Do not post sensitive information on social media. This is often the cause of identity theft.
- Always read and understand online messages and be diligent enough to know and understand the source before clicking anything on the web. This is where identity theft also occur.

As a part of our short and long term plan, we are committed to implement appropriate controls in all areas (People, Process & Technology) of the DepEd IT Infrastructure.

CC: Victoria Catibog, Undersecretary for Finance
Ma. Lourdes Pantoja, Director IV, Bureau of Human Resources and Organizational Development
Francis Allen Dela Cruz, CAO, Personnel Division