Philippine Overseas Employment Administration

Republic of the Philippines
Department of Labor and Employment
BFO Building, Ortigas Avenue cor. EDSA, Mandaluyong City 1501

Website: www.poea.gov.ph E-mail: info@poea.gov.ph
Hotlines: 722-1144, 722-1155

ADVISORY NO. 18
Series of 2021

IMPLEMENTATION OF STANDARD STRONG PASSWORD

In response to the increasing cybersecurity incidents happening in our cyberspace during this time of the Covid-19 Pandemic, this agency will implement counter-measures to secure our cyber and network resources from cybercriminals stalking around the cyberspace to prey on weak and vulnerable government agencies.

One of which is the implementation of having a strong password to gain access to network resources such as office computer, official email addresses/messaging app, online systems, in-house systems, data sharing systems, video conferencing platforms, remote access connection, virtual private network, data administration, system administration.

All passwords should be strong and follow the general guidelines. Making a password strong means increasing its *length, complexity and frequency of changes.*

High risks systems requires strong passwords and supplemented with alternative security measures such as multi-factor authentication (MFA). High risks systems include, but not limited to:

a) Systems that provide access to critical or sensitive information;
b) Controlled access to shared data;
c) Systems or applications with weaker security; and
d) Administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

ICT will reset all passwords and users will be required to input a strong password. General guidelines for a strong password:

1. All passwords must meet the following minimum standards:

   a) Be at least *eight* alphanumeric (alphabet and numbers) characters long;
   b) Contain digits or punctuation characters (e.g. 0-9, ~`!@#$%&()_-'{});
   c) Contain both upper and lower case characters (e.g. a-z, A-Z);
   d) Not be a word in any dictionary or combination of dictionary words;
   e) Not be a word with a number added to the beginning and the end;
   f) Not be solely based on easily guessed personal information, names of family members, pets, birthdays, anniversaries, etc.;

2. To help prevent identity theft, personal identifiable information such as employee name, SSS, GSIS, Philhealth, TIN, bank account or credit card numbers must never be used as a Username/UserID or a password.

3. All passwords are to be treated as sensitive information and should therefore never be shared, discussed, hinted upon, or revealed in forms. Passwords should not be written down or stored online unless adequately secured. *NOTE: Do not use the password feature offered on Windows or other operating systems. This feature creates a password file that is vulnerable to hackers.*

4. Do not use a previous password. If a user account is previously compromised, reusing a password could allow that the user account to once again become compromised.

5. Do not use a single password for multiple accounts. Once the password is compromised, it can have a chain effect allowing an attacker to gain unauthorized access to multiple systems.

6. It is recommended that passwords be changed at least once every thirty days (30) days for general accounts.

7. Passwords that could be used to access sensitive information must be encrypted in transit. Password transmitted in plaintext can be easily intercepted by someone with malicious intent. Secure alternatives include transmitting passwords via encrypted tunnel (e.g. IPSec, SSH, SSL).

For strict compliance.

BERNARD P. OLALIA
Administrator

CONTROLLED AND DISSEMINATED
BY CRD ON JAN 28 2021

296-5