University of the Philippines

OFFICE OF THE VICE PRESIDENT FOR DIGITAL TRANSFORMATION

MEMORANDUM NO. PAS 25-04

TO	**:**	**Chancellors, UP Tacloban College Dean, UP PGH Director**
SUBJECT	**:**	**SECURING OUR WEBSITES AND ONLINE ASSETS**
DATE	**:**	**10 JUNE 2025**

Recent cyber threats underscore the urgent need to collectively fortify our digital infrastructure. I am reaching out to request your partnership in an ongoing System-wide cybersecurity enhancement initiative.

We are asking for your support in the following critical tasks within the next 60 working days. These are essential in strengthening our collective digital security.

1. Domain and Subdomain Inventory
Please provide a complete list of the domains and subdomains your CU hosted or managed in a spreadsheet. For each, include information on (a) domain name, (b) purpose, (c) DNS hosting details (cloud/on-premise, provider) department or unit directly responsible, (d) primary contact person, and (e) email address.

This inventory will help us understand our full digital footprint.

2. Personnel Roster
To help coordinate support and training opportunities, please share an updated list of your units' webmasters and system administrators. We hope to provide the necessary training and orientation where needed. For each individual, include their (a) full name, (b) contact information, (c) most recent cybersecurity training details (including date, title of the training, and training provider or platform), and (d) backup or alternate contact, if available or applicable.

Please download the templates in this link (links.up.edu.ph/ovpdxmemopas2504) and email the accomplished files to cio@up.edu.ph with the subject line: "[Your CU] - Website Security Inventory Submission 2025" by **September 5, 2025.**

3. Security Compliance

UP websites need to achieve at least an "A" grade on both SecurityHeaders.com and ssllabs.com/ssltest. This means implementing proper Content Security Policy, HTTP Strict Transport Security (HSTS), and other related security headers, as well as having the correct Secure Sockets Layer (SSL) configuration. Unmaintained, or noncompliant websites shall be removed from our domain name systems (DNS) or blocked by our firewalls. Please urge your system administrators and webmasters to test their sites accordingly.

4. Cleanup of compromised pages with unauthorized content

Please urge your webmasters and system administrators to conduct a comprehensive audit to identify and remove linkjacked or compromised content from your sites. Webmasters should:

- Search for unauthorized content using Google search queries like: *site:yourdomain.edu.ph casino*
- Identify pages with gambling, pharmaceutical spam, or other malicious links
- Remove compromised pages immediately from your servers
- Submit removal requests to Google Search Console and other search engines
- Implement stronger access controls to prevent future compromises

This cleanup protects our institutional reputation and prevents our domains from being penalized by search engines.

We understand this requires significant work. We stand ready to help with implementation and connect you to relevant experts. After implementation, we will schedule regular check-ins with your IT teams to help maintain security standards and foster continuous improvement.

Should you have concerns or queries, feel free to reach out to OVPDx-ITDC (sechelp@up.edu.ph).

Cybersecurity is a shared responsibility. By working together, we help protect the entire UP community. Thank you for your partnership in this important work.

Peter Sy
PETER A. SY
Vice President for Digital Transformation

Audit trail

Details

FILE NAME	[OVPDxExMemo04] Securing our Websites and Online Assets_v01 - 6/10/25, 7:32 AM
STATUS	🟢 Signed
STATUS TIMESTAMP	2025/06/09 23:34:29 UTC

Activity

▷ SENT	dxstaff@up.edu.ph **sent** a signature request to: • Peter Sy (pasy@up.edu.ph)	2025/06/09 23:32:17 UTC
✍ SIGNED	**Signed** by Peter Sy (pasy@up.edu.ph)	2025/06/09 23:34:29 UTC
✓ COMPLETED	This document has been signed by all signers and is **complete**	2025/06/09 23:34:29 UTC

The email address indicated above for each signer may be associated with a Google account, and may either be the primary email address or secondary email address associated with that account.