WEB HOSTING SERVICE OPERATING PROCEDURES AND PROCESSES

UNIVERSITY COMPUTER CENTER
UNIVERSITY OF THE PHILIPPINES DILIMAN

Document Control

Document Properties

Title	Web Hosting Service Operating Procedures and Processes
Author	Gerardo Maria Roxas
Document Type	Administrative Document
Filename	Web Hosting SOP.gdoc
File location	UPCC/IT Security

Version History

Version Number	Version Date	Author/Modified By	Description
0.01	October 15, 2018	Gerardo Maria Roxas	Initial Version

Table of Contents

Overview

The Computer Center maintains a basic web hosting service that is available for UP Diliman academic and administrative units free of charge. The hosting service has the following technical characteristics:

1. Runs either Apache 2.2 or Nginx
2. Runs PHP 5.4, with newer servers running PHP 7.2
3. Runs MySQL, with 1 database available upon request.
4. The Computer Center can pre-install CMS sites such as Wordpress upon request.
5. The hosting service is shared, meaning multiple sites can be hosted in a single server.
6. End users normally have access only through FTP.
7. FTP and Database access is available only within the Diliman Network (DilNet)
8. Web ports 80 (HTTP) and 443 (HTTPS) are the only ports exposed publicly.

Web Hosting Application Procedures

To apply for this web hosting service, the requesting unit must send a letter to the Computer Center Director endorsed by their head-of-unit (a department chair, project lead, director, dean or the like). The request correspondence must also include the technical point person with his/her contact details. This technical point person will serve as a liaison between the Computer Center and the requesting unit. Once the request has been approved, the Computer Center shall send the initial access credentials to the technical point person.

The Computer Center serves only as a hosting partner; the requesting unit must find its own resources for developing the site.

The site, while under development, shall be accessible only within DilNet to prevent any external compromises while the web site is being developed.

Once site development is complete, the requesting unit shall inform the Computer Center that the site is ready for public viewing. The Computer Center will then perform an initial vulnerability scan of the site to check for any security lapses on the site based on an updated database of vulnerabilities and server security settings.

Once the site has been cleared of initial vulnerabilities, the Computer Center shall make the site available outside UP Diliman and is now viewable globally.

***Important Notice**: The initial vulnerability scan does not guarantee that the web site is 100% free from vulnerabilities - this only means that the site has been cleared of known threats and vulnerabilities from detection tools and methods available during the time scanning. Vulnerabilities and threats may still exist but have not been discovered and exploited yet as of scan time.*

Responsibilities of Requesting Unit on Web Sites:

Units are wholly responsible for the security of their hostings spaces. The websites must observe proper security measures, such as but not limited to the following:

1. Generate and safekeep complex credentials (must be more than 8 characters long, and must contain at least one uppercase letter, a number and a symbol).
2. Update the core Content Management System (CMS) and its plug-ins.
3. Ensure that developers behind plug-ins are actively maintaining their products. Some plug-ins might be compatible with the CMS but are no longer in active development - these means that security patches are not performed and may increase the risk of vulnerability.
4. Maintain proper file permissions on their site folder structure.
5. Perform offline backups of their websites and databases.
6. Report to the Computer Center any security problems they may encounter upon using their site.

Active Threat Scanning and Remediation Plan

The Computer Center performs random network and system security scans every once in a while (at least once a month), whose findings are reported to the Systems and Networks Team. If a security threat from a resource is found, the Computer Center shall report its findings immediately to the requesting unit's appointed liaison for immediate remediation on the part of the requesting unit.

If no action has been performed by the requesting unit despite official correspondences by the Computer Center to rectify these concerns after sixty days, the Computer Center reserves the right to suspend the resource until it no longer poses a security threat. This suspension can only be waived from an endorsement by the UP Data Protection Team.

Once the requesting unit has performed the necessary fixes to their website, the Computer Center shall once again perform a web vulnerability scan on the resource, upon which if no known threats are to be found, the resource shall be reactivated again for public viewing.

Incident Management

Depending on the situation, incidents are handled according to several categories:

1. Cause Origin
    a. Internal (equipment failure, data corruption, human error)
    b. External (DDOS attack, site defacement, natural disasters, etc.)
2. Method of Detection
    a. Monitoring systems deployed by the organization
    b. Reported by persons inside of the organization
    c. Reported by persons outside of the organization
3. Severity of Incident
    a. Mild
    b. Severe

Security-related incidents consist of, but are not limited to the following:

1. *Site defacement* - unauthorized content or pages are inserted upon viewing one or more pages of the website. This includes content that poses as a legitimate site of another but may contain malicious code.
2. *SQL Injection* - unauthorized content, functionality or users are added through the site's database due to an exploited vulnerability in the system.
3. *Distributed Denial of Service* - site response is slow or does not load at all due to a large amount of intentional traffic accessing the site.
4. *Crypto-mining* - unauthorized use of server resources to validate or add transactions in a blockchain digital ledger, usually harnessed through an exploited vulnerability in the system.
5. *E-mail spamming* - using the server's resources to send unsolicited emails to recipients through an exploited vulnerability in the system.
6. *Root access* - unauthorized remote access and control of server resources and processes through an exploited vulnerability in the system.

For most cases, incidents are reported and resolved through the following process:

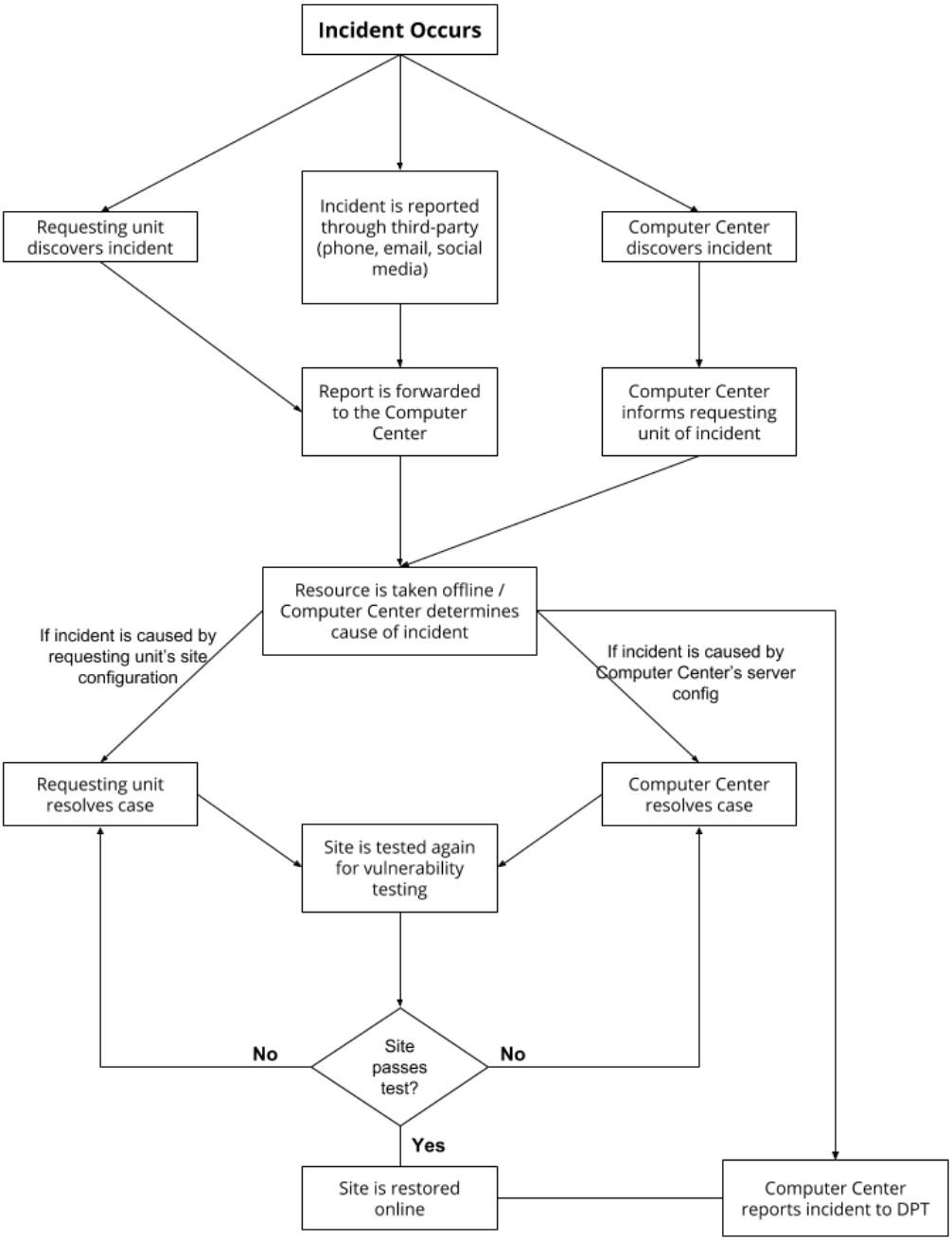

Figure 1: General incident workflow for websites hosted under the Computer Center

Upon discovery of the incident, whether internally by the Computer Center or through another party, the Computer Center shall inform the liaison immediately of the incident.

As a general rule, sites with actively known incidents are immediately taken offline for further analysis. The requesting unit may provide a temporary site or page for the

Computer Center to redirect to; otherwise the site will return an Error 404 page or will be redirected to the default UPD website (https://upd.edu.ph). If the unit has a previous backup of the site and has been updated to address the vulnerabilities that caused the incident, then this can be used to restore the site while the investigation is in progress.

The Computer Center shall perform an analysis to determine the cause of the incident. If the cause was to be found on the website itself, then the Computer Center shall notify the requesting unit of the probable root cause and if possible, the methods to resolve the incident. Examples of causes that are related to the requesting unit are:

1. Out-of-date plugins or Content Management System core.
2. Unpatched known vulnerability of a component in the website
3. Poor coding practices resulting to cross-site scripting or SQL injection.
4. Unsecure passwords that are easily bypassed through brute-force hacking.
5. Leaving folders or files with faulty permissions resulting to unfettered access by remote visitors.

However, there are cases that the cause of the incident can only be rectified by the Computer Center. Examples of these situations are:

1. Out-of-date or unpatched system components with known vulnerabilities, such as the Linux Kernel, Apache, Nginx, SSH and the like.
2. Misconfigured server settings that the regular user does not have access to.
3. Access control configurations (e.g. server and network firewall rules).

Regardless of the party responsible for the resolution of the incident, the resource shall remain offline (or viewable only within DilNet) until a fix is performed by either party. In the case that the requesting unit is the one performing the rectification, they shall notify the Computer Center once they have performed the necessary actions to address the issue. The site shall then undergo system vulnerability testing to check the necessary actions performed has indeed addressed the security incident at hand. If the issue remains unresolved, the Computer Center shall notify the requesting unit that their actions have failed to address the issue, and shall look for a solution to the incident once more. This process will repeat as long as the vulnerability test results flag a security issue with the site.

Once the website passes the vulnerability test, the Computer Center shall once again make the resource available publicly. The requesting unit shall be informed once the site is online and a detailed report to the University Data Protection Team shall be issued.

Credential Retrieval by Existing Users

Forgotten credentials can be reset by sending a message to our support group (support@upd.edu.ph) through the official liaison's email listed on our database. In case a new administrator shall be appointed as a liaison, a letter of endorsement from the unit head shall be required.

Additional Information

The contents of this document may change or be modified without prior notice. Version control is included in the first part of this document.

A condensed version of this document can be found at the Diliman Network website knowledgebase: https://dilnet.upd.edu.ph/kb/webhosting-guidelines/

For comments, corrections and/or suggestions, you may email the University Computer Center at computer.center@upd.edu.ph