Version: 1.6
Effective: December 18, 2014

Annex D - Technical and Security Guidelines on the Government Web Hosting Service (GWHS)

This Technical and Security Guidelines on the Government Web Hosting Service (GWHS) is an annex to the **GWHS Memorandum Circular** of the Department of Science and Technology's Information and Communications Technology Office (DOST-ICT Office).

Content

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

7.3 Service Level Agreement

Annex

Purpose

The Technical and Security Guidelines for GWHS serves as the agencies' guide on migrating to the GWHS and on maintaining their websites. This also includes a checklist that agencies will use during migration.

Security guidelines are also included in this copy to provide the necessary steps that agencies should consider, e.g., what agencies should do before migrating, what they should do if there are vulnerabilities, and what they should do if there are code changes.

Issuing Authority

This document has been compiled and issued by the Department of Science and Technology's Information and Communications Technology Office (DOST-ICT Office) and Advanced Science and Technology Institute (DOST-ASTI) through the Integrated Government Philippines (iGovPhil) Project.

Contact Information

Policies and associated publications under iGov Philippines Project can be found at http://i.gov.ph/.

Queries, suggestions and clarifications with regard to this policy may be forwarded to inquiry@i.gov.ph

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

1. Introduction

The GWHS is an initiative of the Philippine Government to provide for greater security, reliable information, state of the art online services, efficient use of technology, and a robust online network by housing government websites in one hosting service.

The GWHS is one of the components of the Integrated Government Philippines (iGovPhil) Project, which aims to enhance the effectiveness, efficiency, and transparency of the government through the use of interactive, interconnected, and interoperable government applications.

1.1. Objectives

This document provides the guidelines for a seamless migration to the GWHS. It describes a general view of the core infrastructure of the GWHS, outlines the migration procedure, and details the security audit process for a seamless migration to the GWHS. Specifically, this document aims to:

- Give an overview of the GWHS core infrastructure.
- Guide agencies in choosing their web hosting platform.
- Encourage agencies to use the recommended content management systems (CMS).
- Detail the security audit process for migrating sites and sites that are already hosted on the GWHS.
- Outline the migration procedure.
- Describe the operations and maintenance procedures of the GWHS.

1.2. Scope

The Technical Guidelines on the GWHS shall apply to all agencies migrating to the GWHS including:

- National government agencies.
- Government financial institutions.
- Government-owned and -controlled corporations.
- Inter-agency projects.
- State universities and colleges.
- Constitutional bodies.
- Local government units.
- Legislative and judicial branches of the government.

2. Core Infrastructure

The GWHS is envisioned to be a reliable, robust, and secure service that can be easily accessed from anywhere.

The GWHS will be running on two data centers that have the following characteristics:

- Redundant hardware with automatic failover
- Multiple uplinks
- Dual-powered equipment

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

- Generator sets with uninterruptible power supply systems
- Redundant data communications connections
- Environmental controls, such as air conditioning, humidity controls, and fire suppression
- Secure location, installed with biometrics and CCTV systems

The diagram below illustrates the network infrastructure of the GWHS.

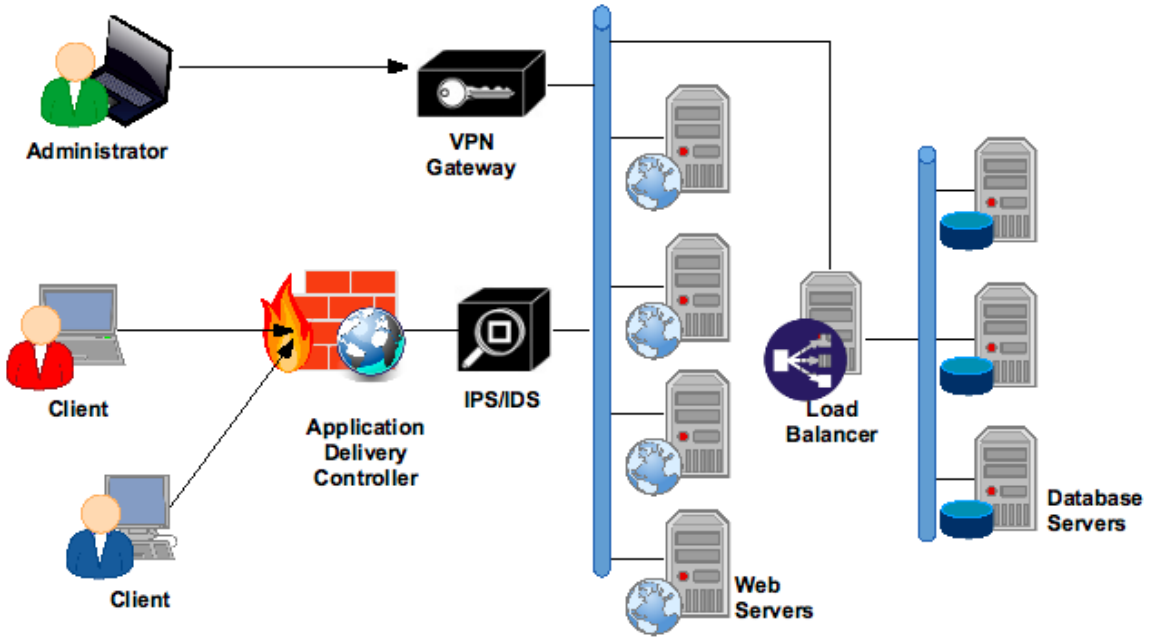

Figure 1. Illustration of the GWHS network infrastructure. Note that this is only a general representation and not the exact configuration of the network, which cannot be disclosed because of security issues.

2.1. Application Delivery Controller

An Application Delivery Controller (ADC) is a device that performs a set of tasks to increase the speed and improve the efficiency of the infrastructure.

The ADC provides the following functionalities:

- Server Load Balancing
- Data Compression
- Caching
- Connection Pooling
- Content-Based Routing
- Traffic Shaping
- SSL Offloading
- Web Application Firewall
- DDOS Protection

The DOST-ICT Office shall be fully responsible for the administration and maintenance of

the ADC.

2.2. Intrusion Prevention and Detection System

The Intrusion Prevention and Detection Systems (IPS/IDS) protect against network and application-level attacks by analyzing network traffic and detecting and preventing anomalous and malicious payloads. The system alerts and notifies the administrators in the event that there are offending IP addresses sending anomalous traffic.

The DOST-ICT Office shall be fully responsible for the administration and maintenance of the IPS/IDS.

2.3. VPN Gateway

A VPN gateway authorizes remote users to gain access to the back-end administrator portal of a website. With a VPN, data is first encrypted and encapsulated before it is sent to the remote VPN server where it is decrypted. This mitigates brute force attacks and unauthorized logins to the back-end portal.

2.4. Load Balancer

A load balancer is a device that acts as a reverse proxy and distributes network or application traffic across a number of servers.

Load balancers are used to increase the capacity and the reliability of applications. They improve the overall performance of applications by decreasing the burden on servers associated with managing and maintaining application and network sessions, and by performing application-specific tasks.

2.5. Web Servers

Web servers on the GWHS shall be using the LAMP stack platform.

LAMP is an open-source web development platform that uses Linux as the operating system, Apache as the web server, MySQL as the relational database management system, and PHP as the object-oriented scripting language.

Administration for websites shall be done through a Unix-based site management panel that provides a graphical interface and automation tools for simplifying the process of hosting and managing websites. This site management panel has such facilities as:

- Webmail access
- Spam filters
- Backups
- Database web management
- Domain name management
- File management
- Application-based support
- Security
- Account statistics

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

For websites using platforms other than LAMP, go to section *3. Web Hosting Specifications*.

2.6. Database Servers

The database servers shall be using MariaDB, an open-source, community-developed fork of the MySQL relational database management system.

MariaDB's features include:

- Synchronous replication
- Active-active multi-master topology
- Reads and writes to any cluster node
- Automatic membership control
- Automatic node joining
- True row-level parallel replication
- Direct clients connections
- Native MySQL look and feel

Database instances shall be administered through the site management panel.

For websites running on databases other than MariaDB, go to section *3. Web Hosting Specifications*.

Note: Agencies interested in the hardware specifications of the equipment running the GWHS, contact the iGovPhil Technical Team through gwtsupport@i.gov.ph.

3. Services Offered and Application Requirements

Aside from the web hosting service, the GWHS also offers the following services:

- .gov.ph DNS registration
- DNS hosting

3.1. .gov.ph DNS Registration

The DOST-ASTI maintains and administers the .gov.ph Domain Registry. For new .gov.ph domain application, .gov.ph domain registry modification, and .gov.ph domain deactivation, visit the .gov.ph Domain Registry website at **http://dns.gov.ph**.

3.2. DNS Hosting

The GWHS also hosts the .gov.ph domains of government websites. For application requirements, visit http://i.gov.ph/ao39.

3.3. Web Hosting

Application requirements for the webhosting service is listed at **http://i.gov.ph/ao39**

IMPORTANT: Agencies migrating to the GWHS shall be required to register three (3) contact persons who will be issued iGovPhil user credentials. These credentials shall be used to create the web space and server space for the agency's website. Likewise,

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

credentials of the contact persons shall be used to access the iGovPhil network service requiring authentication.

Possible contact persons may include:

- the chief information officer
- the head of the MIS division
- web master

User credentials must be renewed yearly.

4. Web Hosting Specifications

Hosting of websites shall be done in two separate environments – Shared Web Hosting and Dedicated or Cloud-based Web Hosting.

Only external or publicly accessible sites or online applications shall be hosted on the GWHS. Internal information systems and applications shall be hosted in-house by the agency.

4.1. Shared Web Hosting

In shared hosting, multiple websites of different agencies shall reside on a single web server and share a common pool of server resources.

Web servers on this shared hosting service shall be running on the LAMP stack platform. Web masters shall be given an administrator account in the site management panel, where users can download pre-packaged distributions of the government web template.

Websites to be hosted on this environment shall be applicable only to:

- Websites using the recommended content management systems (CMS)
- Websites running on Apache, MySQL, and PHP

Table 1. Web hosting specifications for shared hosting

	Shared Hosting
Domains hosted	1
Disk Space	Production Server: 10GB (minimum; can be increased on a per need basis) Development/Staging Server: 500 MB (minimum; can be increased on a per need basis)
Bandwidth	Unlimited
Web Mail	No
Language Support	PHP 5.4, no legacy support
Database Support	MariaDB/MySQL/PostgreSQL
No. of Databases	1

Access/Account in the site management panel	Yes
ssh Access	No
SFTP/FTP Access	No

For websites with online system(s) or application(s), the system(s) or application(s) shall be hosted on a different environment.

4.2. Dedicated or Cloud-Based Hosting

In a dedicated or cloud-based hosting, web masters will be given root access with full administrative access to the server.

Websites to be hosted on this environment shall be applicable only to:

- Websites not using the standard CMS.
- Websites not running on the Linux platform.
- Websites with complex information systems requiring multi-tiered environment.

Websites running outside the LAMP platform shall be housed in a virtual machine in a cloud environment.

Cloud servers will be running on OpenNebula, an open-source cloud computing toolkit, which manages the data center's virtual infrastructure.

The number of domains, disk space, bandwidth, language support, database support, and administrator access shall depend on the resources needed by the agency.

For specific details on cloud-based hosting, refer to the *Guidelines on the Government Cloud*.

4.3. Server Co-location

Agencies that have their own servers have the option to co-locate at the data center of the DOST-ICT Office. The DOST-ICT Office shall only provide power, physical security, and network connectivity. Administration shall be done solely by the agency.

To ensure the security of the GWHS, co-located servers will run on a separate network. DOST-ICTO shall not be held accountable for security breaches on the co-located servers.

Only rack-mountable servers shall be accommodated.

5. Web Content Management Systems

A content management system (CMS) is a software system designed for users with little knowledge on web programming languages to create and manage web content with relative ease.

5.1. Usage

Agencies with existing websites that are migrating to the GWHS are encouraged to use the following open-source CMS:

- Joomla!
- WordPress
- Drupal

These three CMS were selected for the following reasons:

- Cost-effectiveness
- Usability
- Power and flexibility
- Higher security ratings than other open source CMS
- Run on a LAMP infrastructure
- Easier to migrate and secure on the GWHS
- Low learning curve for new users and developers
- Large community support for users and developers

Agencies with no websites are required to use the CMS mentioned above before migrating to the GWHS.

5.2. Distribution

Stable distributions and patch updates of Joomla!, WordPress, and Drupal templates shall be available for download at the http://i.gov.ph/ao39 website or at the iGovPhil Project website (http://i.gov.ph).

It is recommended for all websites to use or update to the latest stable versions of the CMS.

Agencies may expect updates in cases of bug fixes, security fixes, and added features and functionalities to the GWT.

5.3. Modules, Extensions, and Plug-ins

Functionalities of the CMS can be further extended from their basic features and functions. A list of the allowed extensions shall be published at http://i.gov.ph/ao39.

Agencies that want to use extensions not on the allowed list should submit the name or a copy of the extension to gwtsupport@i.gov.ph for a security assessment. Agencies that will develop their own extension shall also submit a copy of the extension to gwtsupport@i.gov.ph for a security assessment.

5.4. Version Control

Version control shall be implemented to track the changes in the GWT. Links to the repository shall be included in the http://i.gov.ph/ao39 page.

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

5.5. Security, Support, and Documentation

Websites using the recommended CMS shall not be subjected to security audits as these CMS and their templates have already been subjected to security audits and assessments prior to official release. However, these websites shall still be subjected to continuous security auditing and shall also follow the procedure on code change requests.

For details on security, go to section *5. Security*.

For support, go to section *6.5.5. Community and Support*

IMPORTANT: Only the recommended CMS shall be supported by the DOST-ICT Office. Maintenance of other systems (proprietary or non-proprietary) and online applications shall be the responsibility of the migrating agency.

User manuals may be downloaded on the iGovPhil Project website (http://i.gov.ph) or at the http://i.gov.ph/ao39 site.

6. Security

6.1. Initial Audit

Initial security checks are necessary to prevent unsecured websites or online applications from compromising the rest of the resources in the web hosting service.

Migration of websites to the GWHS shall follow the testing phase of the security development life cycle.

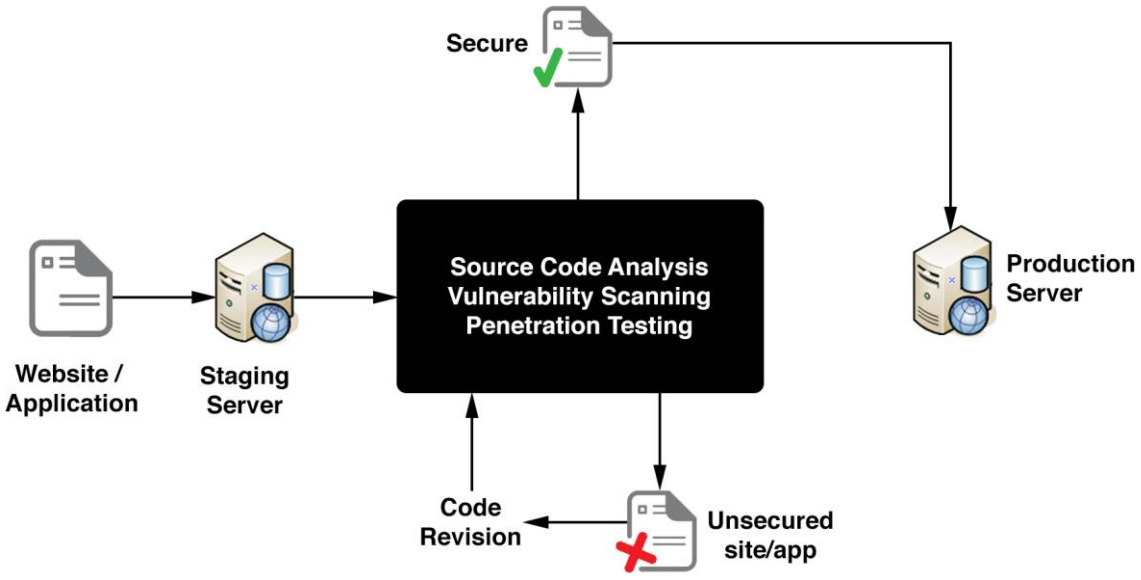

Figure 2. Diagram of the security audit phase.

Websites to be hosted on the GWHS shall be housed first in a staging environment and shall undergo the following security and vulnerability assessment tests to be conducted by the DOST-ICT Office:

- Source code analysis
- Vulnerability scanning
- Penetration testing

IMPORTANT: Agencies using proprietary tools for their website should provide the appropriate license in order to access the code base for security audit and assessment.

As an initial guide for migrating agencies, websites and applications should be compliant to best practices in secure coding and must not have any of the Top 10 risks listed by the Open Web Application Security Project (OWASP).

If a website or an application has been found to be unsecure, the security team shall issue a report detailing the vulnerabilities found and the recommendations and details of where and how the vulnerability was exploited. The migrating agency is expected to fix the vulnerabilities found in the source codes. The site or application will then have to be subjected to another round of security and vulnerability assessment tests until it has been deemed secure for migration by the security team.

Once a site or an application has been deemed secure by the security team, it shall be pushed for release in the production server.

The turnaround time for the initial audit shall depend on the size of the code base and complexity of the source code.

Exceptions to the initial security audit shall only be for websites using the recommended CMS and the official release of their pre-packaged versions.

For the detailed security audit procedure, refer to *Annex A - Security Audit Procedure*.

6.2. Code Changes

All agencies shall update the DOST-ICT Office of upcoming changes to their websites and shall issue a code change request.

Code change requests shall similarly go through the security procedure outlined above and illustrated on *Figure2. Diagram of the security audit phase*. Only source code changes shall go through a change request.

The turnaround time for code change requests is one or two days.

Refer to *Figure 3. Process diagram of the continuous security audit and code change requests*.

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

6.3. Virtual Private Network

Administration of websites shall be done on a secure network accessible only through a virtual private network (VPN). Under no circumstances shall any administration interface be exposed to a public network.

All users logging into the VPN administrative environment shall only use pre-white listed IP addresses submitted to and reviewed by the DOST-ICT Office.

VPN accounts for administration shall be renewed yearly. Only authorized government employees shall be able to have a VPN account. All VPN account users, including web masters, must know basic Linux administration and must undergo basic security training from the DOST-ICT Office. Knowledge on server security and web application security shall be refreshed every three months.

Any administrative or content changes made to government websites shall only be done in secure laptops deployed and configured by the DOST-ICT Office. These laptops shall not provide administrative rights to end-users and shall have full disk-encryption for security. All actions committed by users working on a government website shall be monitored.

All accounts in the site management panel shall only be accessible via VPN. Access shall be given only to requesting agencies and web masters who have undergone the required security training.

6.4. Continuous Auditing

All websites hosted on the GWHS shall be subjected to continuous security auditing and scanning using dedicated bandwidth that shall not hamper availability.

Any website found to have vulnerability shall be disconnected from the network and shall be subjected to change requests until it is safe again to be exposed to the public.

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

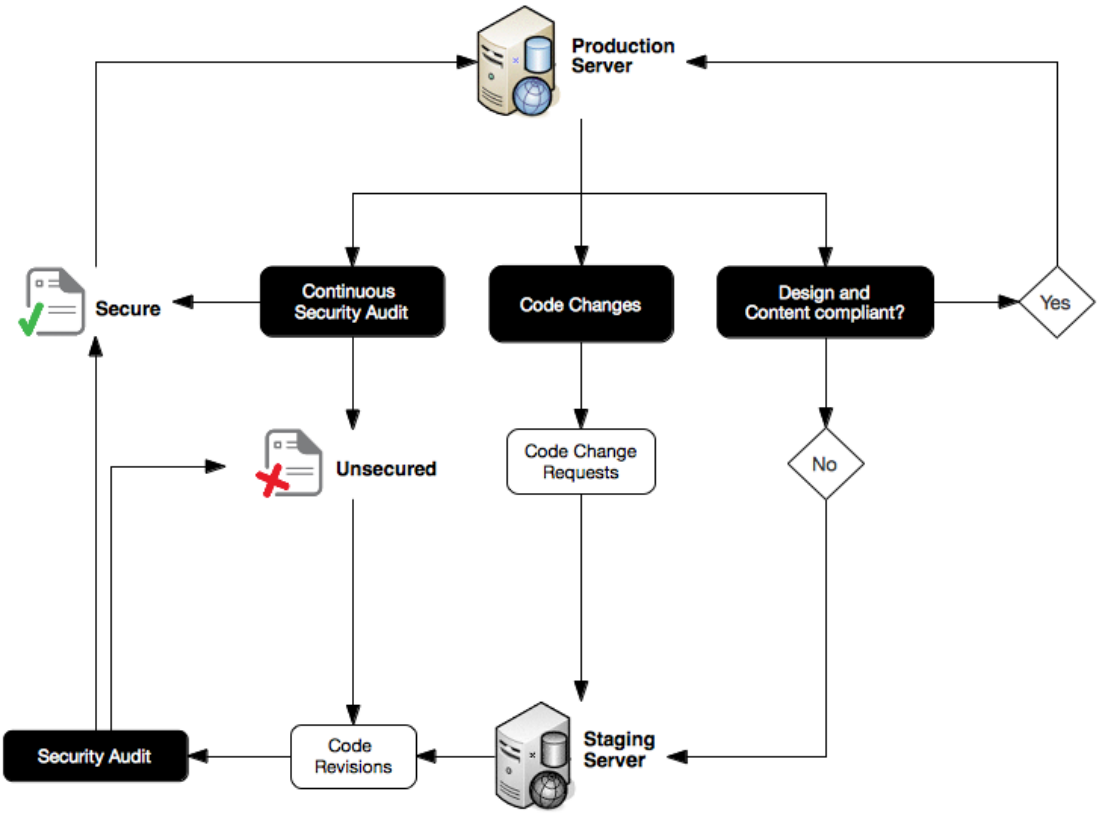

Figure 3. Process diagram of the continuous security audit and code change requests.

7. Migration Procedure

The migration procedure to the GWHS shall take into account the following:

- Answers of the agency in the conducted online website assessment survey.
- Submission of complete application requirements.
- Compliance of the website to the *Government Website Template Guidelines*.
- Security audits of websites not using the prescribed CMS/GWT.

Migration of websites will be done on a first-come-first-served basis.

The diagram below illustrates the steps on how to migrate to the GWHS. The diagram can also be viewed at http://i.gov.ph/ao39.

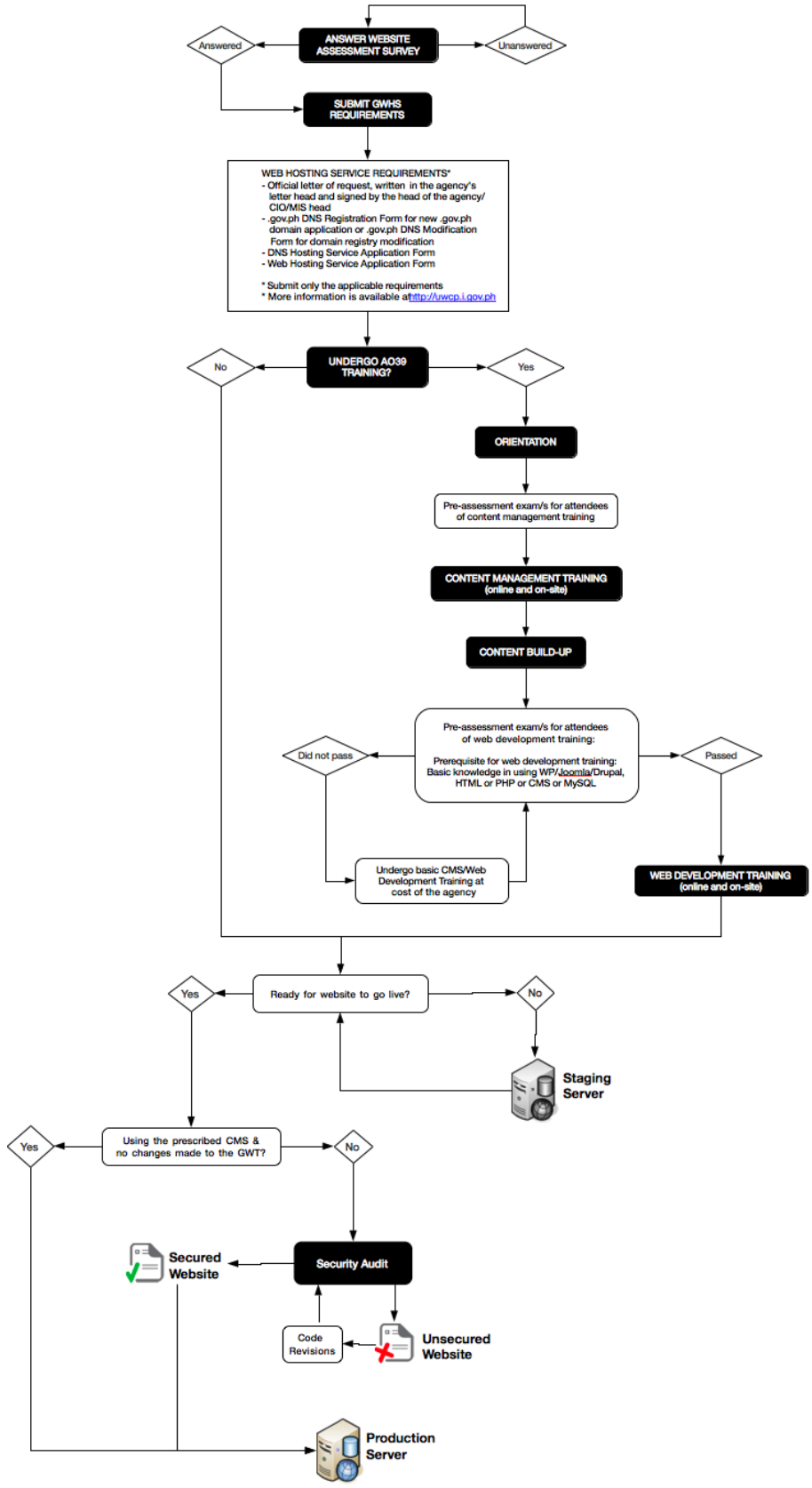

Figure 4. Diagram of the migration procedure

7.1. Migration Checklist

The following checklist shall be used to ensure a smooth and successful migration:

- The agency has responded to the Agency Website Assessment Survey conducted online.
- The website complies with the Unified Web Content Policy.
- The website or online application has passed the security audits and vulnerability assessments.
- The technical requirements for the following have been reviewed and agreed upon by the network administrators of the GWHS and the technical person from the migrating agency:
    - DNS
    - Hosting platform
    - Account access and creation of accounts
    - Upload access
    - Supported languages
    - Hard disk size
    - Database size
- There is a capable technical person from the agency who will do the migration.
- The agency's technical person has been oriented with the features of the web hosting solutions, either by email or in person.
- A date, agreed upon by the migrating agency and DOST-ICT Office, has been set for the migration.

7.2. Operations and Maintenance

The GWHS shall be administered, operated, and maintained by DOST-ICTO 24 hours a day, 7 days a week (24/7).

7.2.1. Administration

Administration of websites hosted on the GWHS shall be done jointly by the agency and DOST-ICTO. Most of the administration, however, shall be done by the agency. Staff of the GWHS shall only take over in cases of security breaches and unforeseen events.

The updating of website contents shall be the sole responsibility of the agency.

Co-located servers are also the sole responsibility of the agency.

7.2.2. Development or Staging Server

A staging server shall be provided to all agency websites hosted by the GWHS. The staging server will serve as the testing platform to any changes to an agency's websites or web applications before it is made accessible to the public.

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

7.2.3. Backup and Resiliency

The network infrastructure of the iGovPhil shall be equipped with redundant hardware components, which shall eliminate single-point-of-failure domains and ensure availability.

Backups and recovery shall run on the Amanda Platform, an open-source backup and archiving software. Backup processes shall be run daily to facilitate recovering unexpected failures and interruption. All backups shall be copied offsite.

Daily backups of the data on the GWHS are for internal operations only. Agencies have the option to maintain a separate backup of their websites and data.

7.2.4. Community and Support

7.2.4.1. Issue Tracking System

Agencies may report technical issues through a help desk that will be implemented with the GWHS. This shall include an issue tracking system and a live chat facility.

7.2.4.2. Online Community

A community site shall be created for agencies looking for ways to get support, learn more, and be involved with the programs of the iGovPH project. This site shall include features such as online chat, online groups, online support, and online forums.

7.2.4.3. Email Support

All queries and concerns can be emailed to the GWHS/GWT support team at gwtsupport@i.gov.ph.

7.3. Service Level Agreement

A Service Level Agreement (SLA) shall be drafted for the migrating agency. Included here will be the specific details of the hosting service needed by the agency and responsibilities of the migrating agency and the DOST-ICT Office.

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

Annex

UN-ASPA Stages of e-Government[i]

Stage	Description	Characteristics
Stage 1: Emerging Presence	The website represents information that is limited and basic.	The e-government online presence comprises a web page or an official website. Links to ministries or departments of education, health, social welfare, labor and finance may or may not exist. Links to regional or local government may or may not exist. Some archived information such as the head of states' message or a document, such as the Constitution, may be available online. Most information remains static with the fewest options for citizens.
Stage 2: Enhanced Presence	The government provides greater public policy and governance sources of current and archived information, such as policies, laws and regulation, reports, newsletters, and downloadable databases.	The user can search for a document and there is a help feature and a site map provided. A larger selection of public policy documents such as an e-government strategy, policy briefs on specific education or health issues. Though more sophisticated, the interaction is still primarily unidirectional with information flowing essentially from government to the citizen.
Stage 3: Transactional Presence	Websites allow two-way interaction between the citizen and government.	This includes options for paying taxes, applying for ID cards, birth certificates, passports, license renewals and other similar C2G interactions by allowing citizens to submit applications online 24/7. The citizens are able to pay for relevant public services, such as motor vehicle violation, taxes, fees for postal services through their credit, bank or debit card. Providers of goods and services are able to bid online for public contacts via secure links.
Stage 4: Connected Presence	The most sophisticated level in the online e-government initiatives.	This can be characterized by an integration of G2G, G2C and C2G interactions. The government encourages participatory deliberative decision-making and is willing and able to

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

		involve the society in a two-way open dialogue. Through interactive features, such as the web comment form, and innovative online consultation mechanisms, the government actively solicits citizens' views on public policy, law making, and participatory decision making.

[i]Web measure model: Stages of e-government evolution (http://unpan3.un.org/egovkb/egovernment_overview/webmeasure.htm)

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

Related Document

Name	Reference	Location
Government Web Hosting Service (GWHS) Memorandum Circular of the Department of Science and Technology Information and Communications Technology Office (DOST-ICT Office)	Integrated Government Philippines Project Website	http://i.gov.ph/

References

Title	Description
Website Migration Plan (June 9, 2013)	General plan on ensuring the smooth migration of a government website to the Government Web Hosting Service (GWHS)
Administrative Order No. 39	Administrative order mandating government agencies to migrate to the GWHS of the Department of Science and Technology-Information and Communications Technology Office (DOST-ICT Office)

Modification History

Version	Effective Date	Changes
1.0	October 2, 2013	
1.1	October 14, 2013	Changes on: 6.2 User Accounts 6.1.1 First Priority 6.5.4 Community and Support Figure 3. Diagram of the migration procedure
1.2	October 21, 2013	Changes on:

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101

		2. Core Infrastructure 3. Web Hosting Specifications 5. Security Added section: 6.6 Service Level Agreement
1.3	November 20, 2013	Changes on: Figure 3. Illustrated diagram of the continuous security audit and code change requests processes Figure 4. Diagram of the migration procedure
1.4	February 11, 2014	Changes on: 7. Migration Procedure Added section: 3. Services Offered and Application Requirements Removed sections: 7.1 Application 7.2 User Accounts
1.5	August 7, 2014	Added disk space information for staging/development and production servers. Added PostgreSQL to list of supported databases. Streamlined and edited for grammar and consistency.
1.6	November 12, 2014	Changed the letterhead

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920-0101