Windows Hosting Environment
University Information Technology Services
Indiana University

Service Agreement
March 2022

2022 CHANGES

- **.NET Framework 4.8 are available in our Windows Hosting Environment.** Send an email to **webhost@iu.edu** for more information.

- **Maintenance windows for the WHE environments have changed.** Windows security updates to stage and production server environments will occur on the Wednesday following the second Tuesday of every month between Midnight and 6 AM. Other maintenance to production environments will occur on Thursdays between 7am and 9am, or Sundays between midnight and 8am. Other maintenance to stage environments may occur at any time; WHE will announce these maintenance periods in advance if they are likely to affect availability of the stage servers.

- **ColdFusion 2016 to ColdFusion 2021 Migration.** WebTech is scheduled to begin transition WHE stage and production sites from the existing ColdFusion 2016 infrastructure to the new ColdFusion 2021 infrastructure during the week of March 28, 2022. All projects should be migrated no later than July 1, 2022. Projects migrated to the new environment will make use of a new portal, **https://cfwhe.iu.edu**. Projects running in the old environment will continue to use the current portal, **https://webhost.iu.edu**, until they are migrated.

- **.NET Migration.** A .NET server migration is planned for Fall 2022.

IMPORTANT INFORMATION AT A GLANCE

- **The Windows Hosting Environment is a baseline service.** There are no fees for internal departments to use the shared hosting environment. There could be fees for additional services such as file restorations and resources such as disk space.

- **A client is required to maintain a developer for each project.** Code and databases that are unable to be maintained to respond to environmental changes will be removed until changes can be made.

- **UITS WHE reserves the right to end service to any application which violates any IU Policy or this Service Agreement,** fails to match environmental upgrade deadlines, or adversely affects the performance of other users.

- **Critical, restricted, and protected data types may be hosted in the Windows Hosting Environment if the owner of the data and UITS WHE grant approval.** Critical data will require the approval of the **IU Data Stewards** before hosting in WHE. **Owners of WHE-hosted critical, restricted, and protected site and/or database content will be required to sign the Service Agreement annually.**

- **PCI DSS v3.0 SAQ A-EP compliance is NOT met on WHE.** Merchant Questionnaires submitted with the assistance of WHE will note areas where policy is not met.

- **Please notify WHE admins if your site has HIPAA requirements, describing your use case.** The Windows Hosting Environment satisfies certain requirements of the HIPAA Security Rule, but can only be used with protected health information (PHI) if you have the complimentary safeguards in place. Please review the KB document **https://kb.iu.edu/d/aqqk** for more information. If the PHI is part of research, please email **securemyresearch@iu.edu** if you have questions about how best to secure it.

- If you are having a problem with the WHE that is not covered by any of the notices on **status.IU**, then please refer to the **Emergency Communications** section below.

- **All system-wide WHE outages will be posted to the Webhost Admin Portal sites at https://webhost.iu.edu and https://cfwhe.iu.edu (for projects migrated to the ColdFusion 2021 environment) on client's project page(s).** We will follow-up with an email to all developers listed in the contacts section of your project. It is up to our clients to make certain this list is up to date for efficient communications.

- **Web applications + sites cannot create or upload files to the project content directories.** If a web application needs a location to create + write files, the client must request a Storage Share location from WHE Admins.

- **All web sites should include a Privacy Notice.** The notice needs to be updated or reviewed at least every two years. For more information, see **https://informationsecurity.iu.edu/resources-professionals/additional-resources/privacy-notice-generator.html** .

OVERVIEW & DEFINITIONS

The Windows Hosting Environment enables clients to use desired technologies not available in any other hosting environment provided by University Information Technology Services, for as low a cost as possible, while maintaining an acceptable level of performance, reliability, and security. Applications requiring other levels of performance, reliability, or security must be hosted elsewhere.

The unique features of this hosting environment are a Microsoft IIS Web Server with the ability to serve dynamic web pages written using Adobe ColdFusion, Microsoft .NET Framework 4.8+ and Microsoft .NET CORE 3.1+ programming languages. WHE also provides a Microsoft SQL Server database environment. The web pages and database servers in this environment can be used with resources outside of the environment.

The Windows Hosting Environment is available to departments on all campuses of Indiana University. The clients develop and maintain the applications, and University Information Technology Services provides the hardware, software, and systems administration.

This environment is provided by the combined efforts of the Enterprise Web Technical Services, Enterprise Windows Administration, and Support Center groups of University Information Technology Services. The remainder of this document describes the environment, and the relationship between the service provider and the service clients.

Our Terminology:

- "Client" refers to the consumer of the services provided by this environment. A client is the organizational unit and all associated individuals served.
- "Provider" or "Service Provider" refers to the University Information Technology Services groups and personnel responsible for providing some aspect of this environment.
- "Workspace" refers to the total scope of a client's use of this environment. A workspace is comprised of all file and database space provided to a client.
- "Project" refers to a sub-grouping of resources within a workspace. A "Workspace" can have one or more "Projects". File and database space are associated with a "Project". The primary reason for multiple "Projects" would be security – to compartmentalize access to files and data to different groups of people.
- WHE: Windows Hosting Environment

THE SERVICE PROVIDER AGREES TO:

- Provide a Windows Hosting Environment 24 hours a day, 7 days a week, except for maintenance and emergencies. See the Guidelines section for further information about scheduled and emergency maintenance.

- Provide a full range of support resources. The service provider responsibilities are divided between the Enterprise Web Technical Services (WebTech) Windows Hosting Environment (WHE) team, Enterprise Windows and Azure Administration Enterprise Server Administration (EWA) , Storage and Virtualization (SAV), and Support Center (SC) groups within University Information Technology Services (UITS).

- The UITS WHE group is the service owner and primary contact for all clients. The UITS WHE group will introduce new clients to the environment, and provide general information to existing clients.

- The EWA group is the database administrator for this environment. The EWA group will install, configure, and maintain the stage and production database software.

- The SAV group will provide virtual servers and allocate additional virtual resources as needed.

THE CLIENT AGREES TO:

SECURE PROJECT WORKSPACE AND DATA

- From the WHE Admin portal, the client must assure "Contacts", "Permissions", and "Access Control Lists" are up to date. "Contacts", "Permissions", and "Access Control Lists" are described in the **Guidelines** and **Access Control** sections of this agreement.

- Inform UITS WHE before you use the environment for critical, restricted, or protected data. For information about data classifications see **https://datamanagement.iu.edu/types-of-data/classifications.php** and **http://kb.iu.edu/data/augs.html**. Additional security measures are required if the site accesses or stores HIPAA or ecommerce PCI DSS data.

MAINTAIN PROJECT WORKSPACE IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT

- The Windows Hosting Environment (WHE) is shared by many clients. In order to provide a maintainable and acceptable level of performance, reliability, and security; the configuration of all applications is standardized. The client may request deviations to the standard but the provider reserves the right to deny any request for customization.

- All client applications must not adversely affect other client applications. **If a client application adversely affects other client applications, the provider may remove the offending client application from service.**

MAINTAIN PROJECT WORKSPACE TO BE COMPATIBLE WITH ENVIRONMENT UPGRADES

- **The client is responsible for making any changes necessary to their application to get it to function in the patched, updated, or upgraded environment.** Often software components in our environment will be patched, updated, or upgraded.

- **A client is required to maintain a "developer" for each project**. Projects that are unable to be maintained to respond to environmental changes will be removed.

- **A client is required to patch/modify/edit code to bring it to a working state.** In some cases environmental changes will make previously working code fail to execute / display properly. The WHE Admins may be able to assist with additional logs, error codes, etc.

- If an environmental upgrade or policy change forces a change of hostname, server operating system, database version, or programming language, the service provider will provide a timeline for this change. The timeline will be reasonable, but non-negotiable.

USE THE FOLLOWING PROCEDURES TO MAKE CHANGES

- UITS WHE is composed of stage and production environments. Best practice is to develop in the staging environments and adequately test in this environment before moving changes to the production area. Only tested code should be applied to the production area.

- For timely production deployments for web applications and databases, WHE admins must be given ample notice by sending an email to **webhost@iu.edu**. Failure to plan a new deployment could result in a delayed launch date.

- Each time a new site is deployed or code is updated, the client must perform a web application security scan in the stage environment before the application will be placed into production. For instructions on how to request a scan see **https://informationsecurity.iu.edu/resources-professionals/additional-resources/website-scanner.html**.

- Significant changes to the production environment (database or file content) should be preempted by an additional web application vulnerability scan against modified test data.

- Other changes can be made by submitting a request to **webhost@iu.edu**. Requests must clearly specify the changes desired. The actual completion date and time will be determined upon review of each individual request.

- The client must notify the WHE Admins of any anticipated "significant" changes in usage, such as a dramatic user base increase or the need for a dramatic increase in disk space, in order to ensure the environment has the resources to accommodate the changes.

FAILURE TO MEET THESE EXPECTATIONS WILL RESULT IN ACTIONS NECESSARY TO ELIMINATE THE RESULTING PROBLEM OR RISK. IN MOST CASES THIS WILL RESULT IN A SITE OR DATABASE BEING TAKEN OFFLINE UNTIL SECURITY CONCERNS ARE MET, OR AN ALTERNATIVE HOSTING LOCATION IS IDENTIFIED.

INITIATING SERVICE

- All new requests to WHE can be submitted to our email address **webhost@iu.edu** or via our online forms: **https://webhost.iu.edu/noclient.cfm** (for those projects in the ColdFusion 2016 environment) **https://cfwhe.iu.edu/noclient.cfm** (for those projects in the ColdFusion 2021 environment)

- Include a proposed name for the client, project and the network ID and email address for the primary contact.

- Additional information that you can share, such as your additional contacts, your programming language, a description of the project function, and the project's data classification **https://datamanagement.iu.edu/types-of-data/classifications.php** will speed up the initial process.

- Development workspaces are available within a week.

ENDING SERVICE

- The client may end their use of the service at any time. UITS WHE reserves the right to end service to any application which violates any IU Policy, this Service Agreement, fails to match environmental upgrade deadlines, or adversely affects the performance of other users.

- When a client ends their use of the service, the provider will archive all files on the production file share and a complete backup of the production database, and a copy of the archive will be made available to the client upon request. The provider will keep a copy of the archived Project for one year.

EMERGENCY COMMUNICATIONS

- The current status of UITS systems and services is available at **status.IU.** If a client is having a problem with a WHE application, that is not covered by any notices on **status.IU** or the WHE Admin Portal , then please follow the guidelines listed below:

  1. In case of an emergency, the client must first consult their developer to resolve the problem.
  2. If the problem cannot be resolved by the client's developer, then the client may contact **webhost@iu.edu** for assistance. If the report is made during normal business hours, then the problem will be investigated. If the problem is reported outside of normal business hours, then the problem will be investigated the next business day.
  3. If a problem with production is identified outside of business hours, then clients or users may contact your **Campus IT Support Center.** If immediate elevation is required, then developers may report the problem to **DC Operations.** The Support Center or Operations will report the problem to the System Administrators. The System Administrators will only be able to perform high level functions such as restarting a problematic server. Do not contact the Support Center or Operations for problems with a stage environment outside of business hours. Instead email **webhost@iu.edu** and the problem will be addressed during the next business day.
  4. When clients or users report a problem to **webhost@iu.edu**, Operations, or the Support Center, the following information is needed:
     - That the application is part of the Windows Hosting Environment.
     - The name of the application.
     - The name, email address, and phone number of who to contact during troubleshooting.
     - A description of the problem, including details such as:

- The complete URL to the problem page.
- The UNC path to the share containing the file with the problem.
- The server and database name if the problem is a database connection.
- A description of the aberrant behaviors.

- You may refer your users to the KB article **http://kb.iu.edu/data/arrv.html** for instructions for user problem reporting for the Windows Hosting Environment.

- All system-wide WHE outages will be posted to **https://status.iu.edu**. We will follow-up with an email to all developers listed in the contacts section of your project as soon as possible. It is up to our clients to make certain this list is up to date for efficient communications.

VIRUS PROTECTION

- Clients are responsible for assuring their files do not contain viruses, malware, or other code insecurities.

- The service provider will provide a log of file changes to assist the client.

- The service provider may periodically scan files for viruses.

DATA BACKUP

- UITS SAV's CommVault service is used for backups and restores.

- Files are backed up as detailed in the SAV Service Level Expectations Document (**https://kb.iu.edu/d/bdyo#3.2.3**).

- "AllDisk" backups will be performed on Virtual Machines (VMs) as defined in **https://kb.iu.edu/d/anep** .

- Clients with backup needs beyond that offered by SAV are responsible for assuring those needs are met.

DATABASE BACKUPS

- A SQL Server full backup of each database is performed daily and written to a file server.

- A SQL Server transaction log database backup of each database is performed daily for production databases only and written to a file server. Transaction logging is not conducted for development databases.

- Production backups are kept for 30 days. Non Production backups are kept for 14 days. All backups are stored on an EWA file server. Additionally, two days worth are kept locally on the database server.

- Clients with backup needs beyond that offered by the default SQL Server backups are responsible for assuring those needs are met. Additional backup and retention accommodations may result in additional fees.

DATABASE REQUESTS

- To restore a back-up of a client database send a request to **webhost@iu.edu** with the source database server name and date of the back-up to be used, and the target database server of the back-up. A database restore will replace the target database.

- Due to the complexity of some database designs, it may not always be possible to move individual objects from one WHE database to another (for example, if a table has multiple dependencies) as these moves are extremely time-consuming and can place the client's data at risk. In these cases, it is incumbent upon the client to provide a script for reassigning any special attributes the object may possess (most commonly – identity, foreign keys, triggers, and/or primary keys).

- WHE admins will work with EWA to perform all backup/restores.

DATA RESTORATION

- Send requests to restore files and databases to **webhost@iu.edu**. Provide the server name, database name or file name and path. Include the last "known good" date.

SCHEDULED JOBS

- All customer scheduled job requests in Windows and ColdFusion, must be reviewed, accepted and set up by the WHE admins. All jobs will need to be scheduled to provide for optimal server performance. Job times will be agreed upon by the customer and WHE Admins.

- This also applies to SQL Server Integration Services (SSIS) packages. Any resource intensive SSIS packages running after 8am on a weekday, that is having a negative impact on the WHE environment, may be terminated at the service providers' discretion. The service provider will make every effort to contact the affected client before, or immediately after, the SSIS package has been terminated.

- SQL jobs and SSIS packages in WHE must adhere to a naming convention specific to our environment. To find out more about setting up SSIS packages and SQL jobs please contact **webhost@iu.edu**.

SCHEDULED MAINTENANCE

- Windows security updates to stage and production server environments will occur on the Wednesday following the second Tuesday of every month between Midnight and 6 AM. The servers or affected services will be down for only the amount of time necessary for the updates.

- Other maintenance to production environments will occur on Thursdays between 7am and 9am, or Sundays between midnight and 8am.

- Other maintenance to stage environments may occur at any time. Whenever possible WHE will announce these maintenance periods in advance if they are likely to affect availability of the stage servers.

- Non-Windows updates will be announced at least three days in advance to affected WHE clients. Any maintenance likely to affect the availability of production servers will be performed outside of normal business hours if possible. Whenever possible these updates will be applied in advance to stage environments to allow time for testing.

- Non-scheduled production maintenance activity will be listed at **status.IU** in addition to the Webhost Portal, and presented at UITS Change Management in some instances.

EMERGENCY MAINTENANCE

- Emergency maintenance will occur as needed. The first priority will be to prevent service loss or to restore service. Consequently, emergency maintenance may be performed without advance notice to clients. Clients will be notified of the emergency maintenance as soon as possible, before or after, as the situation allows.

- A System Administrator is on call 24 hours a day, 7 days a week for production environments. During an emergency the system administrator will give their best effort to restore service. However, there is no guaranteed response or recovery time during an emergency.

- Problems and emergency maintenance activity will be listed at **https://status.iu.edu**

VIRTUAL HOST NAMES & DATA ENCRYPTION

- Virtual host names and SSL certificates are available upon request. The client is responsible for obtaining approval for domain names. For the DNS policies see **http://kb.iu.edu/data/aqeo.html** .

- By default all volumes at rest and network communications between servers are encrypted.

WEB APPLICATION VULNERABILITY SCANS

Windows Hosting Environment web sites must be scanned by the UISO Web Vulnerability Scanner. A scan must also be done to any new sites or major revisions, or annually. Clients will be responsible for requesting the scan and working with UISO to resolve any vulnerability exposed. For instructions on how to request a scan see **https://informationsecurity.iu.edu/resources-professionals/additional-resources/website-scanner.html** .

IT IS ADVISED ALL SECURITY SCANS BE DONE IN A STAGE ENVIRONMENT OUTSIDE OF BUSINESS HOURS AND PRE-COORDINATED WITH UITS WHE. IF A DATABASE REFRESH IS NEEDED BEFORE OR FOLLOWING A SITE SCAN, YOU MAY MAKE THIS REQUEST TO WEBHOST@IU.EDU.

FEES

- No fee for shared web hosting.

- Additional disk space fees:
    - All workspaces include 10 GB of disk space. The space includes:
        - Script, image, and data files on file share
        - Database data and log files
        - Development, test, and production
    - The cost for additional disk space is provided on the UITS Rate List located here: **https://kb.iu.edu/d/apjw#rate** under Disk Storage, and Data backup sections of the document.
    - Charges for additional file spaces are based on average monthly usage during the previous fiscal year.

ACCESS CONTROL

CONTACTS AND CLIENT ACCESS TO THE ENVIRONMENT

- The client must designate at least one individual as a contact for all matters related to use of this service. The provider will only act on requests made by or approved by a designated contact.

- The client must provide a developer contact for all projects.

- The client is completely responsible for controlling access to their workspace.

- The client is responsible for assuring anyone with access to their workspace understands their responsibilities stated in this service agreement.

- The client is responsible for developing and maintaining their content for the entire application life-cycle.

- The client is responsible for adapting their application to changes to the environment such as software and hardware updates and upgrades.

- NTFS and database access is controlled by Active Directory (ADS) domain groups. The groups have the following naming convention – "ADS\IU-WH-Clientname-ProjectName_Developers".

- The Project ADS group has Change permission on the file content (NTFS) directories.

- Web applications/sites cannot create or upload files to the code content directories. If a web application needs a location to create + write files, the client must request a Storage Share location from WHE Admins. Space requirements will be discussed at the time of the request. Critical data may not be stored on the WHE Storage Shares. This is non-negotiable and abuse of this rule will result in termination of access to this share.

- The Project ADS group has db_owner role permissions on development and non-critical production database environments.

- The project ADS group has db_datareader + db_datawriter roles on the critical production database servers. Production databases with a critical classification can only have permissions elevated during a change, or for the duration of 1 week, whichever is shorter.

- The project –Owner local SQL login will have db_datareader + db_datawriter permissions only in all environments.

If other groups, permissions, or database server logins are needed they can be requested.

WEB SITE AND VIRTUAL DIRECTORY SETTINGS

- Each web application will have its own application pool running as a Group Managed Service Account managed by UITS WHE.

- If other web site and virtual directory settings are needed they can be requested.

IU Login

- UITS WHE supports the use of IU Login for limiting access to web pages, using CAS or SAML protocols. See **https://kb.iu.edu/d/atfc** for more information.

- UITS WHE may be able to provide code samples for popular security procedures upon request.

APPENDIX 1 - ADDITIONAL DOCUMENTATION & RESOURCE

WHE Administration Interface in ColdFusion 2016 Environment: **https://webhost.iu.edu**

WHE Administration Interface in ColdFusion 2021 Environment: **https://cfwhe.iu.edu**

IT Security Office Web Application Vulnerability Scan: **https://informationsecurity.iu.edu/resources-professionals/additional-resources/website-scanner.html**

Indiana University Data Classifications: **https://datamanagement.iu.edu/types-of-data/classifications.php**