Appendix 1

CONTENTS

Changes and Important Information................................................................. 2
Overview & Definitions ...................................................................................... 2
The service provider agrees to: ......................................................................... 3
The client agrees to: ......................................................................................... 3
  Secure their workspace and data ................................................................. 3
  Maintain their workspace in accordance with the terms of this agreement. ........................................... 3
  Maintain their workspace to be compatible with environment upgrades ................................................. 3
  Use the following procedures to make changes ......................................................................................... 4
Guidelines ........................................................................................................ 5
  Initiating Service .......................................................................................... 5
  Ending Service ............................................................................................. 5
  Emergency communications ........................................................................... 5
  Virus Protection ............................................................................................ 6
  Data Backup .................................................................................................. 6
  Database Backups ......................................................................................... 6
  Database Requests ....................................................................................... 6
  Data Restoration ........................................................................................... 6
  Scheduled Jobs ............................................................................................. 6
  Scheduled Maintenance ............................................................................... 7
  Emergency Maintenance .............................................................................. 7
  Virtual Host Names & Data Encryption ......................................................... 8
  Web Application Vulnerability Scans ........................................................... 8
Fees .................................................................................................................. 8
Access Control ................................................................................................ 8
  Contacts and client access to the environment ................................................ 8
  Web Site and Virtual Directory Settings ....................................................... 9
  Central Authentication Service (CAS) ............................................................ 9
Appendix 1 - Additional Documentation & Resources .................................... 9
The Windows Hosting Environment is a baseline service. There are no fees for internal departments to use the shared hosting environment. There are fees for additional services such as file restorations and resources such as disk space.

Critical, restricted, and protected data types may be hosted in the Windows Hosting Environment if the owner of the data and WebTech WHE grant approval. Critical data will require the approval of the IU Data Stewards before hosting in WHE. https://datamanagement.iu.edu/governance/data-stewards/index.php

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.

This Windows Hosting Environment has completed the official UITS requirements for HIPAA self-certification. In addition, each use of HIPAA data requires self-certification by the account owner. Please notify WHE admins if your site has HIPPA requirements.

The current status of UITS systems and services is available at https://status.iu.edu. 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 Site at https://webhost.iu.edu 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.

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 and Microsoft .Net programming languages. The environment includes a Microsoft SQL Server database server. 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 Web Administration, Computer Operations, 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.

“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. So 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 compartment access to files and data to different groups of people.
THE SERVICE PROVIDER AGREES TO:

- Provide the 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 Server Administration (EWA), Storage and Virtualization (SAV), Computer Operations (OPS), and Support Center (SC) groups within University Information Technology Services (UITS).

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

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

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

  - The OPS group also monitors server activity and will report problems as necessary to the system administrator.

  - The Support Center will provide first tier support for the environment.

THE CLIENT AGREES TO:

SECURE THEIR WORKSPACE AND DATA.

- 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 WebTech 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. Special note needs to be made if the site accesses or stores HIPPA or ecommerce (PCI DSS) data.

MAINTAIN THEIR WORKSPACE IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT.

- The Windows Hosting Environment 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 does adversely affect other client applications, the provider may remove the offending client application from service.

MAINTAIN THEIR WORKSPACE TO BE COMPATIBLE WITH ENVIRONMENT UPGRADES.

- Every software component employed in the environment will be patched, updated, or upgraded promptly. The client is responsible for making any changes necessary to their application to get it to function in the patched, updated, or upgraded environment.

- To that end, a client is required to maintain a “Developer” contact for each project. Projects in a static state, or that are unable to be maintained to respond to environmental changes will be removed.
• In some cases environmental changes will make previously working code fail to execute / display properly. It is the client’s responsibility to patch/modify/edit code to bring it to a working state. The service provider may be able to assist with additional logs, error codes and the like.

• 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.

• The Windows Hosting Environment is composed of stage and production environments. The client must develop only 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.

• The first time files are moved into “production”, clients must submit a change request to webhost@iu.edu at least two weeks in advance. The actual date and time will be determined by the client and provider at least one week in advance. The client must also have a web application security scan performed in test before the application will be placed into production. For instructions on how to request a scan see https://protect.iu.edu/online-safety/tools/website-scanner.html.

• The first time database objects are moved into “production”, clients must submit a change request to webhost@iu.edu at least two weeks in advance. The actual date and time will be determined by the client and provider at least one week in advance.

• Significant Changes to the production environment (database or file content) should be pre-empted by an additional web application vulnerability scan against modified Test data.

• Other changes can be made by submitting a change 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 provider 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.
Guidelines

Initiating Service

- Express interest to WebTech WHE using the support email address (webhost@iu.edu).
- Include a proposed name for the 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. WebTech 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. 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 https://status.iu.edu. If you are having a problem with the WHE that is not covered by any notices on Status.IU, then please follow the guidelines listed below:
  - In case of an emergency, the client must first consult their developer to resolve the problem.
  - 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.
  - If a problem with production is identified outside of business hours, then clients or users may contact the Support Center (see http://kb.iu.edu/data/abxl.html). If immediate elevation is required, then developers may report the problem to DC Operations (see https://dcops.iu.edu/contactus.php). The Support Center or Operations will report the problem to the System Administrator. The System Administrator 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 test and development outside of business hours. Instead email webhost@iu.edu and the problem will be addressed during the next business day.
  - 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 the Webhost Admin Portal Site at https://webhost.iu.edu 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.

**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)
• 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.
• The backup files are kept for 5 days on the file server. In addition to immediate access to 5 days of backups from the file server we have the SAV backups of the file server (as described above).
• 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 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).
• Temporary elevation of production level permissions to database owner can be granted if the client wishes to move these objects.

**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.
• Restorations may result in additional fees.

**SCHEDULED JOBS**

• To avoid conflicts with backups and scheduled maintenance, Operating system, ColdFusion, SQL Server, and any other jobs targeting the production servers in this environment must be scheduled to not conflict with the production server backup and scheduled maintenance.
- Backups and scheduled maintenance on production servers occurs from midnight to 6am (8am on Sundays). Therefore, scheduled jobs will not be allowed during these times.

- To avoid conflicts with backups and scheduled maintenance, Operating system, ColdFusion, SQL Server, and any other jobs targeting the development and test servers in this environment must be scheduled to not conflict with the development and test server backup and scheduled maintenance.

- Backups on the development servers occur daily from 6 pm to 9.

- Scheduled maintenance occurs Wednesdays from Noon to 5 pm. Therefore, scheduled jobs will not be allowed during these times.

- When job execution periods overlap and server performance is affected, then we may reschedule the jobs involved to spread the load. If this is necessary, then we will work with the affected job owners to reschedule the jobs.

- SQL Server Integration Services (SSIS) packages should be completed before 8am each weekday. Any SSIS package running after 8am on a weekday that is having a negative impact on the WHE environment may be terminated at the service provider’s 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**

- If necessary, security updates to development servers will occur on the Wednesday following the second Tuesday of every month between Noon and 5 pm. If necessary, security updates to production servers will occur between 12am and 8am the following Sunday. The servers or affected services will be down for only the amount of time necessary for the updates – usually for only a few minutes.

- If necessary, other maintenance to development and test servers will occur on Wednesdays between Noon and 5 pm. If necessary, other maintenance to production servers will occur on Sunday between 12am and 8am.

- All other scheduled maintenance will be announced at least three days in advance. Any maintenance likely to affect the availability of the servers will be performed outside of normal business hours if possible.

- Scheduled maintenance activity will be listed at https://status.uits.iu.edu/ in addition to the Webhost Portal.

**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. 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.uits.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](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://protect.iu.edu/online-safety/tools/website-scanner.html](https://protect.iu.edu/online-safety/tools/website-scanner.html)

**IT IS ADVISED ALL SECURITY SCANS BE DONE IN A TEST ENVIRONMENT AND PRE-COORDINATED WITH WEBTECH 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](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 their use of this service. The provider will only act on requests made by or approved by a designated contact.
- The client is completely responsible for controlling access to their workspace.
- The client is also 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 also responsible for adapting their application to changes to the environment such as software and hardware updates and upgrades.

Access is controlled by Active Directory (ADS) domain groups. The groups have the following naming convention – “ADS\IU-WH-Clientname-ProjectName_Developers”. The groups have Change permission on the file shares. The groups have the db_owner role on the development database servers, and the db_datareader and db_datawriter roles on the production database servers.

If other groups, permissions, or database server logins are needed they can be requested. Production Databases with a critical classification can only have permissions elevated during a change, or for the duration of 1 week, whichever is shorter.
WEB SITE AND VIRTUAL DIRECTORY SETTINGS

By default the anonymous web user account has access to all web accessible folders. Each web site, web application, project, or client will have its own application pool running as an ADS account managed by WebTech WHE. This account can also be used to access any database hosted in the environment by request (Integrated Security).

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

CENTRAL AUTHENTICATION SERVICE (CAS)

- The Windows Hosting Environment supports the use of the Central Authentication Service for limiting access to web pages.
- The Service Provider may be able to provide code samples for popular security procedures upon request.

APPENDIX 1 - ADDITIONAL DOCUMENTATION & RESOURCE

WHE Administration Interface: https://webhost.iu.edu

IT Security Office Web Application Vulnerability Scan: https://protect.iu.edu/online-safety/tools/website-scanner.html

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