

**Architecture and Security Technical Standards List**

Original Effective Date: 02/23/04  
Effective Period: 10/03/07 – Current

Release: 1.4  
Status: **APPROVED**

The following is a list of high-level architecture and security standards intended as a tool to be used by the State of Wisconsin Department of Health and Family Services' (DHFS) divisions/offices and the Bureau of Information Technology Services (BITS) when obtaining a vendor's technical proposal and assessing how well it fits the DHFS environment.

When a division/office creates any type of document to solicit IT products or services (such as a Grant Request, Request for Proposal (RFP), Request for Service (RFS), Request for Bid (RFB), or Request for Information (RFI)), BITS will assist in ensuring the technical information is clearly specified and any special handling is identified.

This list should be included in any Request, and the Request should require vendors to respond with a description of how they meet/comply with the requirements listed. Vendors must provide additional information, including version numbers and alternatives, especially where the proposed solution does not fit the applicable standards below.

This list defines the infrastructure within DHFS. This list may be extended if business needs require access from outside of DHFS (such as from the County systems).

When a division/office receives a vendor's response, the division/office should seek the input of BITS in evaluating the response prior to awarding the contract. This will ensure the vendor is in compliance with DHFS' policies and standards, as outlined in this document and on the DHFS WorkWeb (our Intranet site) at: <http://dhfsweb/it/Policies/Policies&Standards/ITPolicy.htm>.

In cases where a division/office has a business need requiring a solution that does not meet with the published DHFS standards and/or policies, BITS can work with the division/office to explore options for acquisition and implementation including assistance in selecting the appropriate vendor and/or products.

Items in { } indicate planned version changes and a probable effective date (by Quarter based on calendar year). It is best to plan for both the current version and the {planned version, date} for each relevant item. **Note:** Planned technologies, version numbers and dates may change.

**Supported Solution Technologies for DHFS:****1) Application Environment:**

- a) Authentication / Identification
  - i) Statewide e-Business Directory (LDAP – Lightweight Directory Access Protocol) [preferred]
  - ii) Novell eDirectory with iChain or MS Active Directory
  - iii) Unique User Ids and Passwords
  
- b) Database
  - i) Oracle v9.i {Oracle v10.g Q1 2008}
  - ii) MS SQL Server 2000 {MS SQL Server 2005 Q1 2008}

**Architecture and Security Technical Standards List**

Original Effective Date: 02/23/04

Effective Period: 10/03/07 – Current

Release: 1.4

Status: APPROVED

- c) Development Platform
  - i) Java, J2EE, OS-independent, browser-independent [preferred]
  - ii) Microsoft .NET, OS-independent, browser-independent
  
- d) Web Server
  - i) IBM HTTP Server v2
  - ii) MS IIS v5
  
- e) Application Server
  - i) IBM WebSphere 5.1
  - ii) MS IIS v5
  
- f) Messaging
  - i) SMTPMail – Sendmail – Unix
  - i) Novell GroupWise v.7 {Microsoft Exchange 2007, Q1 2008}
  - ii) IBM MQ Series
  
- g) Data Transmission
  - i) HTTPS, SSL v3, 128bit
  - ii) HTTP
  
- h) Network Operating System, File and Print Services
  - i) Novell NDS

**2) Desktop Environment:**

- a) Windows XP SP2
- b) MDAC v2.8
- c) Microsoft Office 2003
- d) Novell GroupWise v7 {MS Outlook 2003 Q1 2008}
- e) Internet Explorer v6.0 {Internet Explorer v7.0 Q2 2008}

**3) Server Environment:**

- a) Windows 2003
- b) Sun Solaris

**4) LAN / WAN Environment:**

- a) TCP / IP
- b) SNMP

**5) Mainframe**

- a) Operating Platform: OS390
- b) Database: DB2
- c) Security: RACF

**Architecture and Security Technical Standards List**

Original Effective Date: 02/23/04  
Effective Period: 10/03/07 – Current

Release: 1.4  
Status: APPROVED

**6) HIPAA Compliance**

a) All applications built for programs that must be HIPAA-compliant should reference the requirements published at: <http://aspe.os.dhhs.gov/admnsimp/>.

**7) American with Disabilities Act (ADA) Compliance**

a) All applications should meet the requirements regarding accessibility at the Intranet site <http://www.access-board.gov/sec508/guide/act.htm>.

**8) Access Control Definitions****a) Discretionary Access Control**

A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a user or process given discretionary access to information is capable of passing that information along to another subject.

**b) Role-Based Access Control**

An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform the role.

**9) Deployment Requirements****a) Additional Component Specifications**

- i) Any additional components required for the working of the proposed system must be listed.
- ii) Vendors should include details regarding how their proposed system is compatible with all other components listed in this document.

**b) Deployment Processes**

- i) Vendors should include any information on deployment processes, prerequisites, etc, which may effect the deployment of the proposed system.

**c) Vendors should include capacity requirements for the following:**

- i) Server Disk
- ii) Server Memory
- iii) Transaction Speed/Network Speed
- iv) Client Disk
- v) Client Memory
- vi) Anticipated Growth

**Architecture and Security Technical Standards List**

Original Effective Date: 02/23/04

Effective Period: 10/03/07 – Current

Release: 1.4

Status: APPROVED

**10) Security**

- a) Strong passwords [preferred]
- b) Two-factor authentication [preferred]

See sections on Authentication, Identification, HIPAA, and Access Control for additional requirements.

**11) Hardware**

No non-delegated hardware (contact DHFS IT Acquisition Manager for current list) should be purchased or acquired on behalf of DHFS before being reviewed and approved by the DHFS CIO, if the hardware will be connected to the DHFS network. DHFS hardware standards are suitable for fully supporting the standards listed in this document. Vendors must include hardware requirements in their responses so the solution can be evaluated thoroughly for its fit in the DHFS environment. In some cases, hardware will require a more extensive approval process or an exception before a vendor's solution can be accepted. Hardware outside the DHFS standards noted may be denied. These standards and the contracts available for this procurement change frequently.

See the Desktop, Laptop and Printer Hardware Standards for hardware standards.

[http://dhfsweb/it/Policies/Policies&Standards/3\\_01\\_Desktop\\_Hardware/3-1-pb.pdf](http://dhfsweb/it/Policies/Policies&Standards/3_01_Desktop_Hardware/3-1-pb.pdf)

**12) Problematic Technologies**

Vendors should avoid proposing solutions outside the DHFS standards. Any proposals using the following technologies will need additional justification and review and may be denied. This list is generalized and intended as a guideline only and is not meant to be all-inclusive. Please contact BITS with specific questions.

**a) The following implementations are not compatible with current infrastructure, standards, and best practices:**

- i) Applications requiring a separate account store or directory.
- ii) Applications requiring separate security systems or that do not uniquely identify users.
- iii) Solutions built on operating systems or database platforms not noted above.
- iv) Solutions requiring desktops to have modems.
- v) Solutions with network interface cards bridging a foreign network and the DHFS network.

**b) The following solutions require additional vendor/business justification and/or investigation to determine compatibility:**

- i) Resource-intensive solutions that could potentially exceed the capacity of the network beyond a manageable amount (example: streaming video on the network).
- ii) Solutions requiring remote connection software or desktop client software.
- iii) Applications with highly specialized support requirements.

**Approved by Herb Thompson, DHFS CIO on October 3, 2007**