



# Intranet Application Acceptance Criteria

Author(s): Mary Pearson

Reviewers: Dean Uhlman, Todd King, Galen Bergthold, Mark Kinkelaar, Dan Steen

Approvers: Tina Zapien, Bob Boyd, Paul Stewart, Jim Kersten

## Version History

<b>Date</b>	<b>Version Number</b>	<b>Name</b>	<b>Reason</b>
17 October 2000	1.00	Mary Pearson	Original Policy Creation

## **1. General Information**

### **1.1. Purpose**

This document defines standards regarding the deployment of web-based applications in the Johnson County Intranet environment; specifically applications hosted on the County Intranet servers. These applications may or may not have a data component on an enterprise data server.

### **1.2. Description**

The standards described apply to all applications developed by Johnson County Information Technology services, any custom applications developed by outside vendors, and any off the shelf applications for this environment.

County Departments interested in Intranet Application Deployment should contact the ITS Support Center to initiate the process.

### **1.3. Definitions**

Intranet Application – A web based application, designed to allow users access to County applications and/or data, typically through a browser. Intranet applications execute on Intranet servers on the internal Johnson County network.

MOU – A memo of understanding is an agreement between ITS and another department defining support roles and responsibilities for the Johnson County technology environment.

DNS – Domain Name Services translate URL's such as jocoks.com to the specific network address for that object.

ITS Deployed Application – An application for which ITS has the primary responsibility for development, implementation, and/or support. ITS Deployed applications may be developed by vendors, but are installed, implemented and supported by ITS.

Department Deployed Application – Any application developed by a county department without ITS involvement. This includes off the shelf applications and custom developed software whose selection or development is done outside of ITS. These applications are supported by the originating department.

### **1.4. Roles and Responsibilities**

The Johnson County Information Technology Services department is responsible for the configuration and administration of all County Intranet servers, unless explicitly stated in an MOU. ITS will use the checklist found in Appendix A to ensure compliance with standards.

The ITS Lead Internet Systems Administrator has the overall responsibility for accepting the applications into the production Intranet environment.

Johnson County Departments will be responsible for those tasks as designated in the negotiated memo of understanding (MOU) defining support responsibilities in a joint support situation.

## **2. Deployment**

Future application deployments may present technical reasons for deviating from this standard. Such deviations will be explicitly negotiated by ITS and the deploying department and documented in the memo of understanding.

### **2.1. Application**

Intranet applications reside on an Intranet application server, on the internal Johnson County network. If the application is supported by a department other than ITS, the responsible department will be granted privileges to a defined virtual directory for the application. ITS will manage the Intranet application server.

In addition to the virtual application directory, the department will be responsible for maintaining all code associated with the application. The department will agree to work with ITS during the implementation of infrastructure upgrades that require application changes. All costs associated with code maintenance will be the responsibility of the department.

If the application requires a specific URL, DNS maintenance may be required. ITS will manage all DNS activities.

### **2.2. Database**

In general, there are two scenarios that describe data access requirements for Intranet applications. The major difference in each is the department responsible for the administration of the data store.

Scenario 1: This scenario is described by an Intranet application that accesses a data source on a department maintained server. In this instance, the department may perform all administration of the data store if they wish. They may also choose to have ITS Data Administration group maintain the data store. This will be defined in the MOU.

Scenario 2: In this instance, the Intranet application accesses a data store on an enterprise data server. ITS will manage the server, databases and processes required to refresh data on the enterprise database servers. All data administration tasks will be performed by ITS.

### **2.3. Security**

The deploying department will maintain application specific security. Server related security aspects will be managed by ITS.

### **2.4. Quality Assurance**

Information Technology Services will verify application stability and resource utilization for all applications in the ITS test environment prior to installation in production. Stability and utilization will be verified again once the application is implemented in the production environment. Based on QA results, ITS has the right to reject or remove the application from the production environment until performance issues have been successfully resolved to the satisfaction of ITS.

### **2.5. Documentation**

Intranet applications are required to have full documentation regarding configuration of services and registry changes made during installation. In addition, the department will provide general, technical and volumetric information regarding the application.

### **2.6. Deployment Windows**

ITS will designate deployment time frames to limit disruption to the production environment. Deployment windows may be outside of normal working hours.

## **3. Licensing**

### **3.1. ITS Deployed Applications**

Custom and off the shelf applications installed in the Johnson County Intranet environment will comply with all licensing agreements as designated by the vendor. For ITS deployed applications, ITS will be responsible for ensuring licensing compliance. ITS will also ensure compliance with all database licensing requirements.

### **3.2. Department Deployed Applications**

Departments that support Intranet applications will supply proof of licensing to ITS for both applications and databases as required by the vendor of the product.

## **4. Problem Resolution**

### **4.1. ITS Deployed Applications**

Information Technology Services will be responsible for the resolution of problems associated with applications deployed on the Intranet.

#### ***4.2. Department Deployed Applications***

An application hosted by ITS in the Intranet environment cannot be supported solely by a single department outside of Information Technology Services. Problem resolution procedures will be defined in a memo of understanding (MOU) will be negotiated between ITS and the supporting department.



### Appendix A

This checklist will ensure all applications deployed in the Intranet environment have met the standards defined in this document. Different ITS groups are responsible for verifying the standards as indicated in the checklist.

<u>Standard</u>	<u>Comments</u>	<u>Responsible group</u>	<u>Verified by</u>	<u>Date</u>
Application License Compliance		Infrastructure		
Database License Compliance		Data Administration		
Enterprise Database Server Database Configuration		Data Administration		
Memo of Understanding		Infrastructure		
Documentation		Infrastructure		
Application Server Configuration		Infrastructure		
Quality Assurance – Test Environment		Infrastructure		
Quality Assurance – Production		Infrastructure		
DNS Maintenance		Infrastructure		