



Internet Application Acceptance Criteria

Author(s): Mary Weitzel

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

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

Version History

Date	Version Number	Name	Reason
17 Sept 2000	1.00	Mary Weitzel	Original Policy Creation

1. General Information

1.1. Purpose

This document defines standards regarding the deployment of web based applications in the Johnson County Internet environment.

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 Internet Application Deployment should contact the ITS Support Center to initiate the process.

1.3. Definitions

DMZ, Demilitarized Zone – A logical partition of the Johnson County network, designed to segregate servers, data, and applications accessible by external users from the remainder of the network.

Firewall – A specific device on the Johnson County network whose purpose is to connect networks and control security in communications between networks. The Information Technology Services department maintains, configures and manages firewalls on the Johnson County network.

Internet Application – An application, typically browser based, designed to allow external users access to County applications and/or data.

Port – A mechanism on the firewall device through which a process or application passes. A separate port number is designated for each service running on the system.

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

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 completely 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 assets operating in the DMZ, 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 Internet 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

2.1. Application

Internet applications will reside on an application server, in the DMZ. 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 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.

For applications with specific registered domain names, the ITS Lead Internet Systems Administrator must be designated as the technical contact

2.2. Database

In general, there are three scenarios that describe data access requirements for Internet applications. The major difference in each is the user community performing the most on line transaction processes on the data.

Scenario 1: External customers requiring read-only Internet access. In this situation, the data will be replicated or copied from its original source on the Johnson County internal network and reside on a database server within the DMZ.

Scenario 2: External customers using on online transaction processing (OLTP), update requests from external sources. Again, this data will reside in the DMZ. It may be

replicated to the internal network for integrity reasons.

Scenario 3. Employees requiring access both internally and through the Internet, majority of updates come from the internal network. One example of this type is the current Outlook/Exchange environment. These databases reside on the internal network.

ITS will manage the server, databases and processes required to refresh data in the DMZ. ITS will also have administrative rights to the original data sources for purposes of managing the DMZ assets.

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.

2.3. Security

ITS will manage security on the county firewall server. ITS Security will designate which ports on the firewall will be used for database access by applications.

Application specific security will be maintained by the deploying department. 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

Internet 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 Internet 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 Internet 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 Internet.

4.2. Department Deployed Applications

An application in the Internet environment cannot be supported solely by a single department other than 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 Internet 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		
DMZ Database Configuration		Data Administration		
Data Replication		Data Administration		
Memo of Understanding		Infrastructure		
Documentation		Infrastructure		
Firewall Configuration		Security		
Application Server Configuration		Infrastructure		
Quality Assurance – Test Environment		Infrastructure		
Quality Assurance – Production		Infrastructure		
Domain Name Registration		Infrastructure		