 Plan

[**Agency**]

**Prepared for**

[**Agency**]

Draft Version Number 1

July 16, 2009

**Prepared by**

[**Document author or authoring department**]

**Contributors**

[**Agency Gov 2.0 Coordinator**]

Microsoft Federal Team

**INSTRUCTIONS FOR USING THIS DOCUMENT**

This document contains Microsoft recommendations and typical policies for Gov 2.0 governance. Throughout this document, you will find boilerplate text based on best practices that you can use as is or revise as needed. Look for fields and optional policy information enclosed in square brackets **[ ]**, which you can replace with your organizational information. Instructions for using sections of this document are also enclosed in square brackets.

**Revision and Sign-Off Sheet**

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Version** | **Change Reference** |
|  |  |  | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Reviewers**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Version Approved** | **Position** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |

**Sign-Off**

|  |  |
| --- | --- |
|  |  |
| [**CIO or other executive**] | Date |

|  |  |
| --- | --- |
| **Sign-Off** |  |
| [**Gov 2.0 Coordinator or other sponsor**] | Date |

**Contents**

[1 Executive Summary 1](#_Toc234287373)

[2 Introduction 2](#_Toc234287374)

[2.1 Objective 2](#_Toc234287375)

[2.2 History 2](#_Toc234287376)

[2.3 Audience 2](#_Toc234287377)

[2.4 Scope 2](#_Toc234287378)

[2.5 Responsibilities 3](#_Toc234287379)

[2.6 Risks and Concerns 3](#_Toc234287380)

[2.7 Gov 2.0 Negotiated Terms of Service 4](#_Toc234287381)

[3 Resources 5](#_Toc234287382)

[3.1 Team Roles and Responsibilities 5](#_Toc234287383)

[3.2 Strategy Team 5](#_Toc234287384)

[3.3 Tactical Teams 6](#_Toc234287385)

[3.4 Gov 2.0 User Group Team 9](#_Toc234287386)

[3.5 Gov 2.0 External Go-Live Team 10](#_Toc234287387)

[3.6 On-Premise Equipment 11](#_Toc234287388)

[3.6.1 Required Server Roles 11](#_Toc234287389)

[3.6.2 Required Servers 12](#_Toc234287390)

[4 Project and Operational Management 13](#_Toc234287391)

[4.1 Communication Plan 13](#_Toc234287392)

[4.1.1 Communication to the Organization 13](#_Toc234287393)

[4.1.2 Communication to the Governance Teams 13](#_Toc234287394)

[4.1.3 Communication About Internal Roles and Teams 13](#_Toc234287395)

[4.2 External Go-Live Plan 14](#_Toc234287396)

[4.2.1 Memorandum of Agreement of Appropriate Use and Etiquette 14](#_Toc234287397)

[4.3 Sponsorship 15](#_Toc234287398)

[4.3.1 Sponsorship of Internally Hosted Services 15](#_Toc234287399)

[4.3.2 Sponsorship of Externally Hosted Services 15](#_Toc234287400)

[4.4 Internal Deployment Process 15](#_Toc234287401)

[4.5 Internal Change Management Process 16](#_Toc234287402)

[4.6 Service Level Agreements 16](#_Toc234287403)

[4.6.1 Internally Hosted Systems 16](#_Toc234287404)

[4.6.2 Externally Hosted Systems 18](#_Toc234287405)

[5 Deployment and Go-Live 19](#_Toc234287406)

[5.1 Overview 19](#_Toc234287407)

[5.2 Branding 19](#_Toc234287408)

[5.3 Security 19](#_Toc234287409)

[5.3.1 Internally Hosted Services 19](#_Toc234287410)

[5.3.2 Externally Hosted Services 19](#_Toc234287411)

[5.4 Technology Requirements 20](#_Toc234287412)

[5.4.1 Data-Mining and Analytic Tools 20](#_Toc234287413)

[5.5 Network Impact 20](#_Toc234287414)

[5.6 Compliance Impact 21](#_Toc234287415)

[6 Operational Concerns 22](#_Toc234287416)

[6.1 Operational Uptime and Downtime 22](#_Toc234287417)

[6.2 Operational Quotas 22](#_Toc234287418)

[7 Education and Training 23](#_Toc234287419)

[7.1 Training Requirements 23](#_Toc234287420)

[7.2 Social Fatigue Awareness 23](#_Toc234287421)

[7.3 Liability and Responsibility 24](#_Toc234287422)

[APPENDIX A Staffing Assignments 25](#_Toc234287423)

[A.1 Strategy Team 25](#_Toc234287424)

[A.2 Tactical Operations Team 25](#_Toc234287425)

[A.3 Tactical Training and Support Team 25](#_Toc234287426)

[A.4 Tactical Integration and Development Team 26](#_Toc234287427)

[A.5 Gov 2.0 User Group Team 26](#_Toc234287428)

[A.6 Gov 2.0 External Go-Live Team 27](#_Toc234287429)

[APPENDIX B Server Deployment 28](#_Toc234287430)

[B.1 Wiki Server 28](#_Toc234287431)

[B.2 Blog Server 29](#_Toc234287432)

[B.3 Video-Sharing and Podcasting Server 30](#_Toc234287433)

[B.4 Micro-Blogging Server 31](#_Toc234287434)

[B.5 RSS Server 32](#_Toc234287435)

[B.6 Social Networking Server 33](#_Toc234287436)

[B.7 Mashup Server 34](#_Toc234287437)

[B.8 Presence Server 35](#_Toc234287438)

[APPENDIX C Social Media Policy 37](#_Toc234287439)

[APPENDIX D Go-Live Memorandum of Agreement 38](#_Toc234287440)

1. Executive Summary

The Gov 2.0 Governance Plan is designed to help guide employees and divisions to the governance standards for using and deploying the social media technologies known as *Gov 2.0*.\* This document outlines the planning, deployment, training, security policy, administration, maintenance, best practices, and support needed to launch and support ongoing [**Agency**] use of internally deployed Gov 2.0 capabilities and externally hosted Web 2.0 services. It identifies lines of ownership for both organizational and technical teams, defining who is responsible for various areas of the system. Moreover, this document defines rules and guidelines instituted to provide [**Agency**] staff enough flexibility and control to use and manage Gov 2.0 solutions. It also establishes rules for the appropriate usage of the [**Agency**] Gov 2.0 environments to achieve the following:

* Establish prudent and acceptable practices regarding the use of Gov 2.0.
* Ensure compliance with applicable rules, guidelines, and instructions.
* Educate individuals who may use Gov 2.0 tools and capabilities about their responsibilities associated with such use.
* Help protect employees from any legal repercussions associated with the use of Gov 2.0 tools.
* Ensure employees’ awareness of appropriate online behavior and etiquettes.
* Safeguard [**Agency**] confidential and sensitive data by ensuring that the rules and policies are understood and followed.
* Delineate goals and objectives associated with the use of these newer technologies so that [**Agency**] efficacy and constituent satisfaction are increased.
* Create procedures and standards that enable users and divisions to fulfill their organizational needs in a timely manner.

Establish Gov 2.0 tool standards for social networking.

\*For more information about Gov 2.0 technologies, see [Social Media and Web 2.0 in Government](http://www.usa.gov/webcontent/technology/other_tech.shtml) or search [USA.gov](http://www.usa.gov/) for *social media* or *Gov 2.0*.

1. Introduction
	1. Objective

The primary objective of this document is to establish a governing document for the usage and management of our Gov 2.0 capabilities. Other objectives are as follows:

1. Identify stakeholders who can provide strategic insight, offer direction, and drive initiatives into their respective offices.
	1. Formalize a stakeholder virtual team.
2. Identify the infrastructure and information technology (IT) resources needed to provide operational support.
3. Designate a support system with appropriate channels of escalation for end users and moderators.
4. Establish initial policies and procedures that govern usage and maintenance of Gov 2.0 capabilities.
	1. History

As part of the “Transparency and Open Government” Presidential Memorandum issued January 21, 2009, all agencies are called to embrace and use Gov 2.0 technologies in an effort to foster greater openness, transparency, accountability, and participation. This document answers that mandate. Created by the [**Sponsoring office**] at [**Agency**], this document offers guidance to employees and divisions about relevant governance standards for using and deploying Gov 2.0 technologies.

For more information about Gov 2.0 technologies, see [Social Media and Web 2.0 in Government](http://www.usa.gov/webcontent/technology/other_tech.shtml) or search [USA.gov](http://www.usa.gov/) for *social media* or *Gov 2.0*.

* 1. Audience

This document [**will**|**should**] be read by all employees and directorates who have an interest in using Gov 2.0 capabilities, whether they be internal or external.

* 1. Scope

This document encompasses all social media tools, features, and capabilities, whether acquired for a fee or free of charge. Furthermore, the scope includes both *internal* and *external* use, which are defined as follows:

* **Internal:** Self-hosted Gov 2.0 capabilities—in other words, applications and services hosted on premise. For the purposes of this document, internally hosted tools are said to be *deployed*.

**External:** Web-hosted or vendor-hosted Web 2.0 capabilities, such as social networking sites. For the purposes of this document, externally hosted tools are said to *go live*.

* 1. Responsibilities

It will be the responsibility of the Program Areas and supporting offices to collectively seek out opportunities to enhance organizational processes and operations. The following points may be considered:

* Whether social networking is improving or hindering [**Agency**]’s ability to be transparent and supporting the goal to become more proactive
* How [**Agency**] can use Gov 2.0 tools to improve organizational processes and reduce inefficiencies and duplication
* Additional infrastructure that may be needed to deliver greatest value
* Areas of the organization that offer the most opportunity for growth through the use of social networking
* Whether social networking can be used to create synergy among divisions and departments
* How [**Agency**] can align its Gov 2.0 activities with the goals of the organization
* How [**Agency**] can be of assistance to and coordinate with other groups working on similar social networking initiatives

The organization’s pain points that may be addressed or relieved by this Gov 2.0 effort

The Program Areas ultimately own the Gov 2.0 tools and capabilities. The IT groups facilitate the use of the social networking environments through the planning, deployment, training, security policy, administration, maintenance, best practices, and support of [**Agency**]’s Gov 2.0 tool(s).

* 1. Risks and Concerns

Effective governance has many requirements and dependencies. The following issues are recognized as risks to the success of this document:

1. Inadequate support from the organizational units that affects ongoing governance
2. Inadequate time to fully educate [**Agency**] employees before their use of Gov 2.0 capabilities becomes widespread
3. Implementation of tools that do not provide adequate security, auditing, and records management
4. User or employee ignorance of [**Agency**] policy
5. Refusal of users to abide by the given policies in this document
6. Lack of policy enforcement
	1. Gov 2.0 Negotiated Terms of Service

The General Services Administration (GSA) has negotiated agreements for Terms of Service with certain social networking, video-sharing, and picture-sharing sites. Table 2-1 enumerates the currently known sites which are approved for use in the performance of government activities as of June 2009. [**Agency**|**Office**] [**does**|**does not**] recognize all these agreements.

[Instructions: Use the following paragraph if your agency does NOT or cannot use these service agreements.]

It was determined by [**authority**] that the current GSA Terms of Service agreement needs [**Insert requirement; e.g. spillage security**]. [**Agency**] [**will**|**should**] work with GSA to update the Terms of Service agreement. Until an update to the agreement is made to address these concerns, only the [**Agency**]-approved services in Table 2-1 will be recognized.

For a list of the most current GSA-approved services, see the [Terms of Service agreements](http://forum.webcontent.gov/?page=TOS_agreements) at Web Content Managers Forum (<http://forum.webcontent.gov/?page=TOS_agreements>).

|  |
| --- |
| Table 2-1Approved Services |
| **Services with GSA-Negotiated Agreements** | **Services Agreements Negotiated by**  |
| [**List**] | [**List**] |

1. Resources
	1. Team Roles and Responsibilities

The Gov 2.0 capabilities will be managed by three teams:

* Strategy Team
* Tactical Team

Go-Live Team

Regardless of the names ascribed to these teams, they will play distinct roles and have distinct responsibilities. For the purposes of this document, the teams will be defined as follows:

* Strategy Team
* Tactical Operations Team
* Tactical Training and Support Team
* Tactical Integration and Development Team
* Gov 2.0 User Group Team

Gov 2.0 External Go-Live Team

* 1. Strategy Team

This team will consist of horizontally aligned organization and technology experts who will provide insight into the use of Gov 2.0 capabilities and direction for their advantageous deployment [**both internally and**] externally. Their roles and responsibilities are summarized in Table 3-1. They will be specifically responsible for seeking integration and synergistic points between internal and external Gov 2.0 capabilities. They [**will**|**should**] balance the needs of the organization and IT, weigh the advantages of hosted services versus on-premise capabilities, and compare commercial products to capabilities [**Agency**] can develop. This team will be drawn from a small group of volunteers and reconstructed on a quarterly basis to maintain a fresh perspective on evolving needs and to exploit the collective wisdom of [**Agency**].

|  |
| --- |
| Table 3-1**Strategy Team** |
| **Role** | Provide strategic insight and direction for Gov 2.0 technologies. |
| **Duration** | Four months. |
| **Who** | Peers from across the organization representing a good balance between organizational mission and IT. |
| **Responsibilities** | Drive strategic initiatives into the team members’ respective organizations.Find ways to improve organization processes using Gov 2.0 capabilities.Understand the benefits being derived from Gov 2.0 use.Propose ways to use Gov 2.0 to reinforce goals of transparency, accountability, and participation.Understand the challenges being faced by employees across the organization with the new Gov 2.0 capabilities.Identify synergies with external and internal tools, and propose ways to take advantage of them.Identify the challenges associated with deploying, implementing, using, and integrating internal tools. |

For more information about the people required to staff this team, see Appendix A, [Staffing Assignments](#A_StaffingAssignments).

* 1. Tactical Teams

The Tactical Team consists of three sub-teams charged with supporting the directives of the Strategy Team: Operations, Training and Support, and Integration and Development.

* **Operations:** IT resources responsible for operational support for the Gov 2.0 capabilities deployed in the enterprise. Their roles and responsibilities are summarized in Table 3-2. They [**will**|**should**] help drive system governance, management, and operational resiliency (that is, backup and redundancy). Additionally, they [**will**|**should**] provide an operational impact report of the cost of deploying new Gov 2.0 capabilities; an analysis of compliance with [**Agency**] security guidelines; and an estimate of costs for servers, licenses, deployment, and additional disk space required for content creation and retention. Lastly, this team [**will**|**should**] be responsible for monitoring usage, key health indicators, the technology road map, and upgrades.
* **Training and Support:** System administrators, helpdesk personnel, and other various support resources. Their roles and responsibilities are summarized in Table 3-3. They [**will**|**should**] create an effective support system with appropriate channels of escalation for end users of the internally hosted Gov 2.0 capabilities. This team [**will**|**should**] respond to application questions, provide user education, fix bugs, and handle other problems requiring issue resolution.

**Integration and Development:** Technically talented people with both the willingness and ability to customize, personalize, and integrate the Gov 2.0 capabilities of record for [**Agency**]. Their roles and responsibilities are summarized in Table 3-4. They [**will**|**should**] seek ways to leverage current collaboration tools and organization systems to address opportunities identified by the Strategy Team. Members [**will**|**should**] range from highly skilled programmers to technically savvy Program Area managers with an overriding technical goal as enumerated in [Table 3-2](#Table3_2).

|  |
| --- |
| Table 3-2**Tactical Operations Team** |
| **Role** | Provide IT-related operational support and maintenance for the internal Gov 2.0 infrastructure. |
| **Duration** | Dedicated, permanent position. |
| **Who** | Infrastructure (IT) resources; local operations teams. |
| **Responsibilities** | Ensure the enforcement of the governance.Identify and set up governance procedures, such as: Quotas. Auditing policies.Manage routine maintenance tasks, such as:Nightly backups.Usage monitoring and analysis.Scheduled task validation.Releases and upgrades that keep the technology current. |

For more information about the people required to staff this team, see Appendix A, [Staffing Assignments](#A_StaffingAssignments).

|  |
| --- |
| Table 3-3**Tactical Training and Support Team** |
| **Role** | Provide support to end users for all self-hosted Gov 2.0 tools deployed on premise. |
| **Duration** | Dedicated, permanent position. |
| **Who** | System administrators, helpdesk personnel, and other various support resources. |
| **Responsibilities** | Create an effective support system with proper channels of escalation.Establish a channel of communication to address common issues, such as:FAQ.Gov 2.0 support community of interest for each tool.Respond to application questions, bugs, and other problems requiring issue resolution.Develop a training plan for each Gov 2.0 tool that is deployed.Create and distribute training collateral material.Provide self-help tools that can be tailored by users and divisions to their needs. |

For more information about the people required to staff this team, see Appendix A, [Staffing Assignments](#A_StaffingAssignments).

|  |
| --- |
| Table 3-4Tactical Integration and Development Team |
| **Role** | Integrate, personalize, and, when needed, customize and use Gov 2.0 capabilities in a manner that fulfills the opportunities identified by the strategy team. |
| **Duration** | Dedicated, permanent position. |
| **Who** | Technically talented people with ability to customize, personalize, and integrate requested and chosen Gov 2.0 capabilities. |
| **Responsibilities** | Ensure that the goals set by the Strategy Team are met in ways that:Decrease systems complexity.Reduce the amount of custom coding required.Reduce the number of separate authentication and identity stores.Lower the need for more resources—management, personnel, hardware, and training.Shorten time to delivery.Make use of existing commercial, off-the-shelf solutions.Integrate with existing systems.Increase the use of capabilities that can be deployed government-wide.Increase security and content management.Make use of systems that already integrate with externally hosted Gov 2.0 capabilities.Manage large change requests, develop new features, and carry out program management while ensuring adherence to standards and goals above.Develop personalized solutions.Leverage external code libraries for each Gov 2.0 tool.Establish a community to share and exchange code libraries and solutions.Establish a community to share ideas and best practices.Find a means of educating all developers about each Gov 2.0 tool’s features so that they can develop solutions faster and easier. |

For more information about the people required to staff this team, see Appendix A, [Staffing Assignments](#A_StaffingAssignments).

* 1. Gov 2.0 User Group Team

This team [**will**|**should**] be responsible for establishing a user group for each externally approved Gov 2.0 capability. Their roles and responsibilities are summarized in Table 3-5. The goal of this team [**will**|**should**] be to enable internal, user-to-user self-help and learning by sharing. [**When possible, internally deployed Gov 2.0 capabilities will be used to fulfill the needs of creating and establishing the User Group communities.**] This small virtual team [**will**|**should**] be reconstructed on a quarterly basis from new volunteers whose goal [**will**|**should**] be to lead and maintain a fresh perspective on the needs, benefits, and mission of the community.

|  |
| --- |
| Table 3-5Gov 2.0 User Group Team |
| **Role** | Support peer-based self-help and learning by sharing. |
| **Duration** | Four months. |
| **Who** | Peers from across the organization. |
| **Responsibilities** | Establish user group communities for each approved, externally hosted Gov 2.0 tool.Moderate discussions and community questions.Share best practices for using the external tools. |

For more information about the people required to staff this team, see Appendix A, [Staffing Assignments](#A_StaffingAssignments).

* 1. Gov 2.0 External Go-Live Team

This team [**will**|**should**] be responsible for helping [**Agency**] adopt a new service in a clear and organized fashion. Their roles and responsibilities are summarized in Table 3‑6. They [**will**|**should**] coordinate the education of [**Agency**] staff about online etiquette and appropriate use of Gov 2.0 services and tools, coordinate the approach [**Agency**] will take in its interaction with the public, and work with appropriate public affairs channels for press announcements.

|  |
| --- |
| Table 3-6Gov 2.0 External Go-Live Team |
| **Role** | To guide, plan, and prepare [**Agency**] and employees to adopt a new Gov 2.0 service so that its rollout is organized and its use understood. |
| **Duration** | One year. |
| **Who** | Peers from across the organization selected by the executive sponsor of the service that is preparing to go live. |
| **Responsibilities** | Educate employees about social media etiquette. Educate employees about appropriate behavior online.Educate employees about how to establish accounts.Educate employees about required security guidelines, including safeguarding passwords and accounts.Generate Memorandum of Agreement (MOA) between employee and [**Agency**] with input from Human Resources. |

For more information about the people required to staff this team, see Appendix A, [Staffing Assignments](#A_StaffingAssignments).

* 1. On-Premise Equipment

All on-premise equipment associated with self-hosted Gov 2.0 capabilities [**will**|**should**] be subject to this governance, except where existing IT governance policy dictates otherwise. In cases of discrepancy, the existing IT governance policy will prevail. Unless otherwise noted, all equipment will be centrally located at [**Consolidated Operations Center**]. Required servers are listed in [Table 3-7](#Table3_7).

* + 1. Required Server Roles

For each type of hosted service, servers [**will**|**should**] be required to support the following:

1. **Production environment:** The configuration used to host the production, working service, including a Web server, federated search server, database server, and SAN array
2. **Development environment:** The configuration that mirrors the production service and hosts the Web and database servers for use by software and Web development teams
3. **Test environment:** The configuration of physical and virtual servers used to test an image of the production and working service

For more information about server assignments, see Appendix B, [Server Deployment](#B_ServerDeployment).

* + 1. Required Servers

|  |
| --- |
| Table 3-7Required Servers |
| **Gov 2.0 Capability** | **Servers Needed** |
| Wiki server | 1. Production wiki server(s)
2. Development wiki server(s)
3. Test wiki server(s)
 |
| Blog server | 1. Production blog server(s)
2. Development blog server(s)
3. Test blog server(s)
 |
| Video-sharing and podcasting server | 1. Production video-sharing and podcasting server(s)
2. Development video-sharing and podcasting server(s)
3. Test video-sharing and podcasting server(s)
 |
| Micro-blogging server | 1. Production micro-blogging server(s)
2. Development micro-blogging server(s)
3. Test micro-blogging server(s)
 |
| RSS server | 1. Production RSS server(s)
2. Development RSS server(s)
3. Test RSS server(s)
 |
| Social networking server | 1. Production social networking server(s)
2. Development social networking server(s)
3. Test social networking server(s)
 |
| Mashup server | 1. Production mashup server(s)
2. Development mashup server(s)
3. Test mashup server(s)
 |
| Presence server | 1. Production presence server(s)
2. Development presence server(s)
3. Test presence server(s)
 |

For more information about specific server roles, names, and IP addresses for our configuration, see Appendix B, [Server Deployment](#B_ServerDeployment).

1. Project and Operational Management
	1. Communication Plan
		1. Communication to the Organization

Communication to [**Agency**] regarding this governance [**will**|**should**] be hosted on a Web site. Its content [**will**|**should**] be accessible from the home page of the Headquarters portal site. There [**will**|**should**] be sections on the page for:

1. Governance overview.
2. What employees need to know about using social technologies:
	1. Gov 2.0 (internally hosted tools).
	2. Web 2.0 (externally hosted tools).
	3. Current organization-approved services.
3. Service level agreements (SLAs).
4. Roles and responsibilities for teams and individuals.
5. Current team membership, as well as instructions for becoming a member.
6. Hardware equipment hosting the environment and its status.
7. Contact information for support, helpdesk, and community.
8. Operational policy.
9. Application usage policy.

In addition, there [**will**|**should**] be an official Gov 2.0 community of interest to help drive improvement, usage, open discussions, and help.

* + 1. Communication to the Governance Teams

Communication to the governance teams regarding this document or any governance activities or issues [**will**|**should**] be in the following forms:

1. Web content as described earlier
2. Gov 2.0 community postings
3. Web-based targeted alerts
4. Scheduled meetings or conference calls
5. E-mail
	* 1. Communication About Internal Roles and Teams

For each Gov 2.0 system, the Tactical Team [**will**|**should**] document, at a minimum, the roles, security, and privileges of the following types of users of the system.

Required roles to be defined for each system:

1. Application administrator
2. Application owner
3. Application member
4. Application moderator
5. Application support
6. Application operator

For each Gov 2.0 system, the following [**will**|**should**] also be documented:

1. Appropriate channels of escalation for end users
2. Responsibility for application questions, bugs, and other problems requiring issue resolution
	1. External Go-Live Plan

The Strategy Team [**will**|**should**] establish the creation of an External Go-Live Team. The purpose of the External Go-Live Team [**will**|**should**] be to coordinate the education of [**Agency**] staff regarding the appropriate use and etiquette for using the target service or tool. They [**will**|**should**] also coordinate the approach taken by [**Agency**] for its interaction with the public and work with appropriate public affairs channels for press announcements.

* + 1. Memorandum of Agreement of Appropriate Use and Etiquette

It is the goal of [**Agency**] that all staff who want to participate in an External Go-Live event and subsequent use of approved externally hosted Web 2.0 sites [**will**|**should**] read etiquette documentation for the related service and establish an account in accordance with [**Agency**] security policy. All employees [**will**|**should**] sign the Memorandum of Agreement (MOA) prepared by the External Go-Live Team. The MOA will outline policies and requirements and require employees who sign up to [**use**|**not use**] their [**Agency**] e-mail address and to identify themselves as [**a | an**] [**Agency**] employee by appending ([**Agency**]) or **-**[**Agency**] to their sign-in or user name (for example, *JoeSmith-Agency)*. In accordance with security policy, the MOA will instruct employees ***not*** to use any variation of their [**Agency**] logon account names or user names associated with Windows®, LDAP, or other special systems or data accounts. The MOA will also instruct employees ***not*** to use current or previously used passwords for any system or logon used by [**Agency**].

Human Resources [**will**|**should**] work with the External Go-Live Team to include guidance on the use of profanity, sexually suggestive phrases or words, and other postings that may reflect negatively on [**Agency**]. The guidance [**will**|**should**] remind employees of the disciplinary results of such actions.

* 1. Sponsorship
		1. Sponsorship of Internally Hosted Services

The Strategy Team [**will**|**should**] review adoption and controls. It [**will**|**should**] solicit feedback from users and executive sponsors of the internal Gov 2.0 applications. See Table 4-1.

Feedback and application effectiveness [**will**|**should**] be presented to [**Agency**] management semiannually with specific focus on addressing realized benefits from the use of Gov 2.0 systems and a list of actions to improve systems.

|  |
| --- |
| Table 4-1Internal Executive Sponsors |
| **Gov 2.0 Application Service** | **Executive Sponsor** | **Planned Deployment Date** |
|  |  |  |
|  |  |  |
|  |  |  |

* + 1. Sponsorship of Externally Hosted Services

For each approved, external social networking or Web 2.0 service used on the Internet, [**Agency**] [**will**|**should**] designate an executive sponsor. See Table 4-2. The purpose of this executive sponsor [**will**|**should**] be to guide [**Agency**] and the Strategy Team in quantifying the value of a given service to [**Agency**], take an active role in protecting [**Agency**]’s reputation, and ensure that its goals will be met by the service.

|  |
| --- |
| Table 4-2External Executive Sponsors |
| **Web 2.0 Service** | **Executive Sponsor** | **Planned External Go-Live Date** |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Internal Deployment Process

The on-premise environment that hosts Gov 2.0 capabilities for [**Agency**] will be deployed as resources and funding become available in order of priority determined by the Strategy Team. Each Gov 2.0 application that is recommended for deployment [**will**|**should**] have an executive sponsor.

The Strategy Team should strongly consider solutions that allow for self-service deployment. Doing so allows greater flexibility, permits fuller employee participation, and lowers maintenance and operations costs. The Tactical Teams [**will**|**should**] provide feedback on the security and protection of information within the proposed systems.

All Gov 2.0 applications [**will**|**should**] be centrally deployed at one or more regional operation centers for the use of the organization in [**worldwide**|**U.S.**] operations.

The Tactical Team [**will**|**should**] analyze the impact to heating, ventilation, and air conditioning (HVAC) systems of new Gov 2.0 application servers on the current centers. They [**will**|**should**] recommend those Gov 2.0 applications that have the lowest impact on the environment, as well as the lowest impact on HVAC and utility costs. In addition, Tactical Teams [**will**|**should**] consider the use of virtual environments, such as Windows Hyper-V™, as a means of reducing hardware expenditures and avoiding unnecessary virtualization and Gov 2.0 application licensing costs.

* 1. Internal Change Management Process

Tracking of changes and versions of configuration to the proposed and deployed Gov 2.0 applications will be the responsibility of the respective Application Administrators and Tactical Operations Team.

Each Application Administrator and Tactical Operations Team [**will**|**should**] propose a system to track changes to the Gov 2.0 applications. Teams should make an effort to leverage owned technologies and processes.

Incremental backups [**will**|**should**] be performed on all applications nightly. A full backup [**will**|**should**] be performed weekly. Should data become deleted accidentally, a request for data restoration can be made through [**Agenc**y] helpdesk. Data recovery for requests older than one week from the deletion event cannot be guaranteed.

Each Gov 2.0 application [**will**|**should**] be tested quarterly for backup and restore operations. Should a real-world system recovery take place, that recovery will satisfy this requirement for testing the backup and restore operations.

* 1. Service Level Agreements
		1. Internally Hosted Systems
1. **Service availability:** Application services will aim for availability 24 hours a day, 7 days a week, with the exception of a scheduled maintenance window. Application services may be made unavailable as needed to perform maintenance during the maintenance window, with appropriate communication and notification. Application services [**will**|**should**] be hosted in [**one or more Operations Centers**] and maintained by [**Agency**|**System Integrator**]. It is recognized that occasionally an unplanned network or server problem may occur that will impact application service availability. Notifications of an unplanned outage [**will**|**should**] be communicated on the home page of the helpdesk Web site [**URL**].
2. **Issue escalation:** All problems shall be reported to the [**Agency**] helpdesk at ([**telephone number**]). Support for application services [**will**|**should**] be available from 8 A.M. to 5 P.M. Eastern Time, Monday through Friday. After-hours support [**will**|**should**] be escalated as defined by the [**Agency**] escalation process and coordinated as needed. Callers must provide the URL of the application service in question. Deviation from the needed information may result in a delay of issue resolution. Problem reporting and service requests [**will**|**should**] be handled on a full-time, around-the-clock basis through the [**Agency**] helpdesk, subject to contracted service hours.
3. **Backup and recovery:** Incremental backups of application services sites [**will**|**should**] be performed nightly. Full backups [**will**|**should**] be performed weekly. Should data be deleted accidentally, requests for data restoration can be made through the [**Agency**] helpdesk. The time required to restore data depends on the complexity of the recovery effort. Data recovery for requests older than one week from the deletion event cannot be guaranteed.
4. **Performance:** As implemented, self-hosted enterprise Gov 2.0 application services [**will**|**should**] be designed to provide performance (for example, usability and response time) consistent with similar Web-based applications operating on the [**Agency**] intranet. Several factors may affect performance, including a user’s location, network bandwidth at the user’s site, and overall network load at the time of use (peak usage times versus off hours). Any user experiencing significant degradation in the performance of self-hosted Gov 2.0 application services should report the problem to the [**Agency**] helpdesk as described [later in this document](#User_Queries). Response to performance problems [**will**|**should**] be handled based on defined severity levels as described [later in this document](#Return_to_service_goals).
5. **Service issues:** Problems affecting components managed by [**Agency**|**System Integrator**] [**will**|**should**] be resolved in accordance with established procedures. [**Agency**] helpdesk logs reported problems using the service desk.
6. **Return-to-service (RTS) goals:** RTS targets [**will**|**should**] be based on the severity of a problem. Recovery targets for issues involving repairs to vendor-supported hardware are affected by the terms and conditions of the applicable vendor service contract(s). In these cases, [**Agency**|**System Integrator**] [**will**|**should**] make every effort to attain the standard recovery goals, but success may be limited due to the vendor’s response capability.
7. **User queries:** For questions about or issues with an application service, users should first contact the designated Gov 2.0 application owner and administrator. If the application owner and administrator are unavailable, or if users detect system problems, the [**Agency**] helpdesk should be contacted.
8. **Query resolution:** The[**Agency**] helpdesk will provide first-call resolution to user questions and problems whenever possible. Problems and service requests that cannot be resolved by the [**Agency**] helpdesk analyst will be routed to the [**Agency**|**System Integrator**] Tactical Operations Team for resolution.
9. **Disaster recovery:** The application service will be offered as a best-effort service at this time. In the event of a disaster, [**Agency and/or System Integrator**] has established [**duration**] [**hour(s)**| **day(s)**| **week(s)**] for recovery time as an internal objective, not a contractual commitment.
	* 1. Externally Hosted Systems

There is no special SLA negotiated with external GSA Terms of Service agreements or services. The service is the responsibility of the commercial/public vendor. [**Agency**] makes no expressed guarantee of any non-[**Agency**] systems.

1. Deployment and Go-Live
	1. Overview

This section provides guidance for deployment of internally hosted Gov 2.0 application services and going live with externally hosted Web 2.0 services. A standard approach [**will**|**should**] be used for application look and feel, regulatory compliance, classification, and schemas for the purpose of supporting system integration and data-mining of the information submitted to Gov 2.0 application systems.

* 1. Branding

[**Agency**]’s branded external site, located at [**URL**], [**will**|**should**] serve as a guide for the look and feel of all external services. [**Agency**]’s branded internal site, located at [**URL**], [**will**|**should**] serve as a guide for the look and feel for all internal Gov 2.0 application services.

Application Service Moderators should label their data in accordance with [**Agency**] standards. Development of Web pages [**will**|**should**] comply with [**Agency**] standards.

* 1. Security

Any security-related incident [**will**|**should**] be reported to the [**Agency**] Information Security Office immediately by the application owner, site administrator, sub-administrator, or user.

* + 1. Internally Hosted Services

If an application service is identified as containing potential security risks, it may be locked to restrict modifications while under investigation. For more information, refer to the Certification and Accreditation document maintained in the Information Security Office.

The Tactical Operations Team and the Information Security Office [**will**|**should**] analyze the authentication model used by a proposed internally hosted application and map it to currently deployed authentication schemas. Preference [**will**|**should**] be given to those systems that reduce the overall management of security by making use of existing implementations and management procedures.

* + 1. Externally Hosted Services

Upon report of a security-related incident, such as posting [**Agency**] confidential information on a public site, the Tactical Operations Team [**will**|**should**] immediately remove Internet access from [**Agency**] to the application under investigation. An e-mail notification [**will**|**should**] go out to all employees, informing them to immediately stop using the site both at work and home. The [**Agency**] Information Security Office [**will**|**should**] contact the moderator and executive sponsor of the site to verify that the security-related issue has been resolved.

When information marked as *classified*, *sensitive*, or *For Official Use Only* is posted to an external site, the Information Security Office [**will**|**should**] initiate an investigation into the sequence of events that led to the posting and make an interim recommendation to all [**Agency**] employees explaining how to prevent the mistake from recurring. The Information Security Office [**will**|**should**] also recommend process changes to the Strategy Team, Tactical Operations Team, and executive sponsor so that such mistakes are prevented when other technology systems are introduced or adopted.

* 1. Technology Requirements

The Strategy and Tactical Teams [**will**|**should**] work with external services to understand Web services and open standards supported by each externally hosted service. For each external system, a technology evaluation report [**will**|**should**] be created and [**will**|**should**] analyze whether the external site allows data-mining of contributions made to the service by the public, employee, and [**Agency**]. Additionally, the Strategy Team [**will**|**should**] document tools for the service that can be used to analyze data and mine for important trends. The Strategy Team [**will**|**should**] evaluate whether those tools meet [**Agency**]’s data-mining and analytics goals.

The Strategy Team and the Tactical Integration and Development Team [**will**|**should**] work to understand the underlying platform’s suitability for use in the [**Agency**] environment, given the existing skills and code base. Special consideration should be given to platforms that already have been deployed within the organization for social networking and to the integration points of the proposed and existing systems.

* + 1. Data-Mining and Analytic Tools

Based on the technology requirements, the Strategy and Tactical Teams [**will**|**should**] investigate and recommend tools for deeper analysis of adopted Gov 2.0 applications and services. The goal of such analysis and data-mining is to drive improvements and proactive response to public or employee input.

For [**Agency**] to take full advantage of external and internal social networking and Web 2.0 interactions, and thereby drive improvements and proactive response to public or employee input, tools outside the freely available sets [**will**|**should**] be considered, as should integrated tools that will allow:

1. Alerts of trends.
2. Alerts and reports of popular topics.
3. Reports of number and speed of posts (that is, topic and conversation pace).
4. Drill-down capabilities for deeper exploration of a root cause or topic.
	1. Network Impact

For each new externally hosted or self-hosted application service, the Tactical Operations Team [**will**|**should**] analyze its network impact using a test environment or pilot deployment. The goal will be to provide a high level of service quality while understanding multimedia bandwidth requirements.

Based on their findings, the Tactical Operations Team [**will**|**should**] make recommendations to reduce the impact of increased network use on day-to-day organizational operations (for example, by offloading e-mail conversations). They [**will**|**should**] explore the cost of additional lease lines, which are needed to accommodate connecting and streaming of multimedia from the Internet. Lastly, they [**will**|**should**] recommend the use of technologies and approaches that can be used to dynamically or statically allow different quality streaming across the LAN or WAN for internally hosted applications.

* 1. Compliance Impact

For each proposed Gov 2.0 application and externally hosted Web 2.0 service, the Tactical Operations Team will rate and evaluate its compliance with the following standards, as appropriate:

1. Section 508 of the Disabilities Act
2. Freedom of Information Act (FOIA)
3. Children's Online Privacy Protection Act of 1998 (COPPA)
4. Federal Advisory Committee Act (FACA)
5. National Institute of Standards and Technology (NIST)

The Tactical Operation Team [**will**|**should**] recommend to the Strategy Team and executive sponsor those solutions that can most closely comply with or achieve these standards. Additionally, preference [**will**|**should**] be given to systems that have already been deployed and have shown compliance and support for these standards.

1. Operational Concerns
	1. Operational Uptime and Downtime

See Section 4.6, [Service Level Agreements](#ServiceLevelAgreement), earlier in this document.

* 1. Operational Quotas

Each application service [**will**|**should**] have a default disk space quota of approximately [**size, in terabytes**]. At any time during the life of the application, this quota can be changed upon request by the application owner, executive sponsor, or their designee.

When the application is approaching this limit, system monitoring software, such as Microsoft System Center, [**will**|**should**] be used to notify the site owner and executive sponsor. If no action is taken in advance, when the application reaches its quota limit, it [**will**|**should**] be set to read-only until the quota is increased. Increases should be requested through the helpdesk.

1. Education and Training
	1. Training Requirements

For any new internally hosted Gov 2.0 or externally hosted Web 2.0 application to be approved, deployed, or used, a solid training plan [**will**|**should**] be required. The goal of the training plan should be to ensure that users will adopt a new service and use it effectively in their daily activities. See Table 7-1 for more training requirements.

|  |
| --- |
| Table 7-1Training Requirements |
| All users of a service [**will**|**should**] receive some form of training. |
| End users [**will**|**should**] receive, at a minimum, overview training in the use of the service. |
| Sponsoring managers [**will**|**should**] be educated about the service, including its capabilities, benefits, and risks. |
| Application owners and site administrators [**will**|**should**] receive advanced training that includes information about office integration and security policies. |
| Helpdesk personnel [**will**|**should**] receive intensive training and troubleshooting analysis.  |
| Training tools may include:1. “How-to” documentation.
2. Instructor-led training.
3. Online labs hosted on a sandbox environment, when applicable.
 |
| The training approach [**will**|**should**] begin with elementary tasks and progress to more difficult tasks, culminating in administrator-level tasks and offering certification. |

Standard computer-based training (CBT) [**will**|**should**] be provided at [**Agency training Web site**] or [**video streaming site**]. The Office of IT [**will**|**should**] conduct mandatory Application Administrator and Application Owner training. Application Administrators and Application Owners [**will**|**should**] take the basic and intermediate CBT training programs.

If CBT does not exist, the Tactical Training Team [**will**|**should**] create and share it internally by leveraging existing tools.

* 1. Social Fatigue Awareness

All employee training should include reference to *social fatigue*, a relatively new phenomenon brought about by the rising use of Gov 2.0 and social media applications. Social fatigue refers to the perception or need to constantly interact with social networks. Awareness of this concept is important to communicate so that employees maintain job satisfaction as they adopt new services. Human Resources [**will**|**should**] work with training teams to raise awareness and help employees build work habits that guard against social fatigue.

* 1. Liability and Responsibility

[**Agency**] legal representatives will work together with the Strategy Team and Human Resources to establish and provide guidance to employees on their liability, indemnification, and responsibility when using an externally hosted Gov 2.0 service.

This policy will be included in the [**Agency]** [training program](#TrainingRequirements) mentioned earlier in this document.

Staffing Assignments

A.1 Strategy Team

The people listed in Table A-1 will form the Strategy Team. Their role will be to provide strategic insight and direction to [**Agency**] on emerging Web 2.0 technologies.

|  |
| --- |
| Table A-1 **Strategy Team** |
| **Region** | **Department** | **Contact** | **Contact E-Mail** | **Contact Phone** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

A.2 Tactical Operations Team

The people listed in Table A-2 will be assigned to the Tactical Operations Team. This team will provide IT-related support and maintenance of the system infrastructure.

|  |
| --- |
| Table A-2**Tactical Operations Team** |
| **Region** | **Department** | **Contact** | **Contact E-Mail** | **Contact Phone** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

A.3 Tactical Training and Support Team

The people listed in Table A-3 will be assigned to the Tactical Training and Support Team. This team will provide support to end users of internally hosted Gov 2.0 applications.

|  |
| --- |
| Table A-3**Tactical Training and Support Team** |
| **Region** | **Department** | **Contact** | **Contact E-Mail** | **Contact Phone** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

A.4 Tactical Integration and Development Team

The people listed in Table A-4 will be assigned to the Tactical Integration and Development Team. This team will integrate and customize all internally hosted Gov 2.0 applications.

|  |
| --- |
| Table A-4Tactical Integration and Development Team |
| **Representing Area** | **Contact** | **Contact E-Mail** | **Contact Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

A.5 Gov 2.0 User Group Team

The people listed in Table A-5 will form the Gov 2.0 User Group Team. This team will set up and manage the user communities associated with externally hosted Gov 2.0 tools.

|  |
| --- |
| Table A-5Gov 2.0 User Group Team |
| **Representing Area** | **Contact** | **Contact E-Mail** | **Contact Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

A.6 Gov 2.0 External Go-Live Team

The people listed in Table A-6 will form the Go-Live Team. This team [**will**|**should**] be assembled by the executive sponsor of an externally hosted service and prepares employees for service adoption.

|  |
| --- |
| Table A-6Gov 2.0 External Go-Live Team |
| **Representing Area** | **Contact** | **Contact E-Mail** | **Contact Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Server Deployment

[Instructions: Below are general server requirements for a reliable and integrated deployment that are platform/product agnostic.]

B.1 Wiki Server

|  |
| --- |
| Table B-1Production Wiki Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web (1) |  |  |
| Web (2) |  |  |
| Federated Search Server (1) |  |  |
| Database (1) |  |  |
| Database (2) |  |  |
| SAN Array (1) |  |  |
| SAN Array (2) |  |  |

|  |
| --- |
| Table B-2Development Wiki Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web |  |  |
| Database Server |  |  |

|  |
| --- |
| Table B-3Test Wiki Environment (Physical and Virtual Servers) |
| **Server Role** | **Physical Server Name** | **Virtual Server Name** | **Physical IP Address** | **Virtual IP Address** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

B.2 Blog Server

|  |
| --- |
| Table B-4Production Blog Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web (1) |  |  |
| Web (2) |  |  |
| Federated Search Server (1) |  |  |
| Database (1) |  |  |
| Database (2) |  |  |
| SAN Array (1) |  |  |
| SAN Array (2) |  |  |

|  |
| --- |
| Table B-5Development Blog Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web |  |  |
| Database Server |  |  |

|  |
| --- |
| Table B-6Test Blog Environment (Physical and Virtual Servers) |
| **Server Role** | **Physical Server Name** | **Virtual Server Name** | **Physical IP Address** | **Virtual IP Address** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

B.3 Video-Sharing and Podcasting Server

|  |
| --- |
| Table B-7Production Video-Sharing and Podcasting Server Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web (1) |  |  |
| Web (2) |  |  |
| Federated Search Server (1) |  |  |
| Database (1) |  |  |
| Database (2) |  |  |
| SAN Array (1) |  |  |
| SAN Array (2) |  |  |

|  |
| --- |
| Table B-8Development Video-Sharing and Podcasting Server Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web |  |  |
| Database Server |  |  |

|  |
| --- |
| Table B-9Test Video-Sharing and Podcasting Server Environment (Physical and Virtual Servers) |
| **Server Role** | **Physical Server Name** | **Virtual Server Name** | **Physical IP Address** | **Virtual IP Address** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

B.4 Micro-Blogging Server

|  |
| --- |
| Table B-10Production Micro-Blogging Server Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web (1) |  |  |
| Web (2) |  |  |
| Federated Search Server (1) |  |  |
| Database (1) |  |  |
| Database (2) |  |  |
| SAN Array (1) |  |  |
| SAN Array (2) |  |  |

|  |
| --- |
| Table B-11Development Micro-Blogging Server Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web |  |  |
| Database Server |  |  |

|  |
| --- |
| Table B-12Test Micro-Blogging Server Environment (Physical and Virtual Servers) |
| **Server Role** | **Physical Server Name** | **Virtual Server Name** | **Physical IP Address** | **Virtual IP Address** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

B.5 RSS Server

|  |
| --- |
| Table B-13Production RSS Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web (1) |  |  |
| Web (2) |  |  |
| Federated Search Server (1) |  |  |
| Database (1) |  |  |
| Database (2) |  |  |
| SAN Array (1) |  |  |
| SAN Array (2) |  |  |

|  |
| --- |
| Table B-14Development RSS Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web |  |  |
| Database Server |  |  |

|  |
| --- |
| Table B-15Test RSS Environment (Physical and Virtual Servers) |
| **Server Role** | **Physical Server Name** | **Virtual Server Name** | **Physical IP Address** | **Virtual IP Address** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

B.6 Social Networking Server

|  |
| --- |
| Table B-16Production Social Networking Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web (1) |  |  |
| Web (2) |  |  |
| Federated Search Server (1) |  |  |
| Database (1) |  |  |
| Database (2) |  |  |
| SAN Array (1) |  |  |
| SAN Array (2) |  |  |

|  |
| --- |
| Table B-17Development Social Networking Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web |  |  |
| Database Server |  |  |

|  |
| --- |
| Table B-18Test Social Networking Environment (Physical and Virtual Servers) |
| **Server Role** | **Physical Server Name** | **Virtual Server Name** | **Physical IP Address** | **Virtual IP Address** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

B.7 Mashup Server

|  |
| --- |
| Table B-19Production Mashup Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web (1) |  |  |
| Web (2) |  |  |
| Federated Search Server (1) |  |  |
| Database (1) |  |  |
| Database (2) |  |  |
| SAN Array (1) |  |  |
| SAN Array (2) |  |  |

|  |
| --- |
| Table B-20Development Mashup Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web |  |  |
| Database Server |  |  |

|  |
| --- |
| Table B-21Test Mashup Environment (Physical and Virtual Servers) |
| **Server Role** | **Physical Server Name** | **Virtual Server Name** | **Physical IP Address** | **Virtual IP Address** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

B.8 Presence Server

|  |
| --- |
| Table B-22Production Presence Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web (1) |  |  |
| Web (2) |  |  |
| Federated Search Server (1) |  |  |
| Database (1) |  |  |
| Database (2) |  |  |
| SAN Array (1) |  |  |
| SAN Array (2) |  |  |

|  |
| --- |
| Table B-23Development Presence Environment |
| **Server Role** | **Server Name**  | **IP Address** |
| Web |  |  |
| Database Server |  |  |

|  |
| --- |
| Table B-24Test Presence Environment (Physical and Virtual Servers) |
| **Server Role** | **Physical Server Name** | **Virtual Server Name** | **Physical IP Address** | **Virtual IP Address** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Social Media Policy

[Instructions: Insert Agency policy letter.]

Go-Live Memorandum of Agreement

[Instructions: Insert Agency Memorandum of Agreement.]