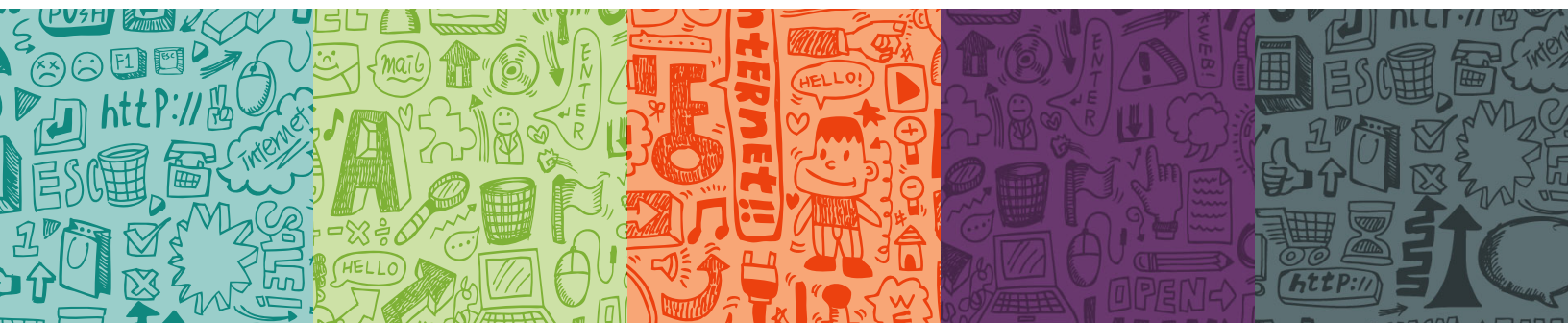
palantir.net

Palantir.net's Guide to Digital Governance



Introduction

In this age of information, digital communications are perhaps the most vital form of outreach an organization has for presenting itself to the world. Today it is probably more likely that a person's first experience or interaction with your organization will occur through the Internet. It is then no wonder that most institutions feel they must have a website or they have to be on Facebook and Twitter. These are now the places where reputations are built and managed.

There are no shortages of services and materials for building a digital presence, whether it is on the web or a social network; however there is less focus on how these presences will be managed and maintained after they are built. This is the all-important and too-often neglected role of digital governance, otherwise known as the ownership, management, and sustainability plan for an organization's various digital communications platforms.

Governance seems simple at a distance — it is the set of rules an organization will follow for its digital communications – but the devil is in the detail, and the details are precisely where the process of defining a governance plan becomes prickly. The details are also where many will become bogged down, lose momentum, and set the plans aside, never to be addressed again until a problem arises.

To help get you started developing a governance plan for your institution's digital communications, I have put together a guide that outlines many of the questions you will want to answer in thinking through policies and guidelines in your governance plan.

The format is literally a series of questions you can answer that will help you begin to consider key issues in digital governance and how you want to handle them.

The guide is based largely on work I have done in higher education, but I have generalized here for broad use across industries.

The guide has sixteen sections that follow a specific order intended to help you start at a high-level of thinking about your digital communications, properties and assets, and then focus on greater and greater levels of detail.

- Scott DiPerna, Director of Production Services

Contents

Starting at the 10,000ft View

Define the digital ecosystem your governance planning will encompass.

When I first begin to think about digital governance for any organization, I like to back up as far as I can to see everything I should include in my planning, or what people sometimes call the 10,000ft view.

Digital communications can encompass many different things, from websites to social networks to broadcast email, so I suggest backing up to the point where you are looking at the various platforms that will be part of your planning.

Here is a list of some common platforms encompassed in a digital communications strategy:

+ Public Websites
+ Private Websites
+ Intranets and Portals
+ Web-Based Applications
+ E-Commerce
+ Social Networks
+ Digital Media
+ Broadcast Email
+ Digital Communications Governance *

This list contains the common "properties" or platforms on which a digital communications strategy is built, or at the very least they are some basic categories for the grouping of such properties.

For instance, your organization may have a main website with many sub-sites or microsites. Others may be combined in your institution; for example, all of your web-based applications may be built within your Intranet site.

Make your own list align with the properties you need to include in your governance plan. These will be your top level categories.

* Few among us would likely think to include "Digital Communications Governance" on this list, but I do so precisely for that reason, and because I want to reinforce that Governance (its documents, people, and processes) is a living thing that needs to be maintained over time, just like the rest of the list.

It's oddly self-referential to think about governance for Governance, but think of it like the part of the Constitution that describes how to amend the Constitution.

Properties and Platforms

Define all the sites, applications, and tools that live in your digital ecosystem.

Having started at the 10,000ft view to assess the digital ecosystem for our governance planning, part two of the Guide to Digital Governance begins to identify the specific properties and platforms you will need to consider within that ecosystem.

Taking the top level categories you listed for your governance plan in part one, you now will want to think of the properties and platforms within each of them. The following questions are intended to help you think through each piece carefully.

Public Websites

- What are the websites we own that are visible to anyone on the web?
- Do we have any public subdomain websites, such as subdomain.mywebsite.com?
- Do we have any micro-sites, or websites with a URL that is different from our main site?
- Do we have any blogs that may be hosted elsewhere, but would be considered part of our public web presence?

Private Websites

- What are the websites we own that are visible to only those with access we control?
- What are the websites we own that are visible to only those who have access through machines running on our organization's network?
- Do we have any subdomain websites, such as subdomain.mywebsite.com that require logging in?
- Do we have any websites for only a specific set of constituents?

Intranets and Portals

- Do we have a network of internal-use websites (a.k.a an Intranet), accessible only by password or by logging on to the organization's network, or otherwise hidden (even by obscurity)?
- Do we use any portal sites or pages as a means of aggregating links of importance for specific groups of users?

Web-Based Applications

- Are there any web-based applications we use to perform specialized tasks, such as generating reports from data in a database or retrieving digital assets from a database?
- Are there any online tools that we use (whether built internally or purchased from a third-party vendor as software-as-a-service (SaaS)?

E-Commerce

- What platforms, systems, and/or services do we use for collecting payments online?
- What platforms, systems, and/or services do we use for selling products (including tickets, donations, etc.) online?
- Where are these hosted relative to our other websites?

Social Networks

+ What are the social media networks we use to communicate to the outside world?

Digital Media

+ What are the platforms we use to create digital media, such as video, audio, and photography?
+ What are the platforms we use to distribute digital media, such as video, audio, and photography?

Broadcast Email

+ What are the systems we use to send broadcast email to all or large segments of our internal group, members, staff, community, etc.?
+ What are the systems we use to send broadcast email to all or large segments of our external community, clients, constituents, etc. for the purposed of marketing and promotion?

Digital Communications Governance

+ What are the pieces that will constitute our official governance system?
+ NOTE: You may not know the answer to this one yet, so leave it empty for now.

Ownership

Consider who is ultimately responsible for each site, application, and tool.

Now that we have defined all of the digital properties and platforms that we will consider for our Governance Plan, we next need to establish who "owns," or who will ultimately be responsible for the care, maintenance, and accuracy, of these properties.

Ownership is the cornerstone of good governance. In fact, some may think of ownership as being synonymous with governance. From my experience, I believe that good governance of any digital communications platform involves more than simply defining who is responsible for each piece.

In most organizations, many people are using, sharing, and collaborating on the same systems together. The processes and interactions between those users needs to be defined as well, however we have to identify the people before the process. Defining ownership first is the foundation on which we can begin to define the more complex relationships that exist in a shared system.

Ownership is the cornerstone of good governance.... Defining ownership first is the foundation on which we can begin to define the more complex relationships that exist in a shared system.

I should make one other important distinction between maintenance of the system and the maintenance of the presentation of content, as it relates to ownership.

Since this Governance Plan is considering the guidelines for digital communications, it is explicitly NOT considering the roles, policies, and procedures for the maintenance of the infrastructure that supports the properties and platforms we are considering for the plan.

In other words, when we define who has ownership of the public website or the Intranet, we are considering only the content and its presentation – not the underlying software and hardware that makes the website or Intranet functional.

Perhaps this is obvious, but it is an important distinction to make for those who are less familiar with modern web technology, who may not fully understand where the functions of an IT department end and an Online Marketing or Communications department begin.

With those caveats out of the way, we can now begin to define who is responsible for each of the properties and platforms we listed earlier.

Obviously, I can't tell you who is or who should be responsible for each piece within your organization – that must be defined by how your work responsibilities are distributed across the institution – but I can describe some general principles for defining ownership that should help.

+ Ownership of your organization's web presences ultimately should reside at the very top, with levels of responsibility being delegated down the hierarchy of the institution.
+ The top leadership of an organization should be responsible ultimately for the accuracy and maintenance of the content contained within the parts of the properties they own.

- Every website, subsite, microsite, department site; every section and sub-section; every page, aggregated listing, and piece of content all the way down to each video, photo, paragraph, headline, and caption should fall within the ownership of someone at the top.
- Responsibility for daily oversight and hands-on maintenance of those properties then may be delegated to staff within the owner's groups, offices, or areas of responsibility.
- Owners should have sufficiently trained staff who have the authority and capacity to make changes, corrections, and updates to the content as needed in a timely manner, such that inaccurate and/or outdated content does not remain on the property for an unreasonable period of time.

In short, ownership has two essential aspects:

1. top-level responsibility for the accuracy and efficacy of the content, and
2. hands-on responsibility for the creation and maintenance of the content.

Both are essential and required for good governance, and very likely may be responsibilities held by one person, split between two, or shared among a group.

Shared Ownership / Responsibility
There may be instances in which shared ownership may be necessary. I generally recommend against doing that as it puts at risk a clear chain of accountability. If two people are responsible, it's easy for both to think the other person is handling it.

If some form of shared ownership is required, consider having one person be the primary owner, who is supported by a secondary owner when needed; or that a primary owner is a decision-maker, but secondary owner(s) are consulted or informed of issues and pending decisions.

If "equally" shared ownership or responsibility is required, try defining the exact responsibilities that are to be owned and dividing them logically between the two. Perhaps there is a logical separation of pages or sections. Or maybe one person is responsible for copy, while another is responsible for images.

Shared ownership is less-than-ideal, but there can be reasonable ways to make it work, provided you do not create any structural gaps in authority, unwittingly.

Collaboration
There are many instances in digital communications where groups of people collaborate to produce content. This is most common with organizational news and events, publications, blogs, social media, etc.

For example, if there is a single person who can be ultimately responsible for all blog content created by various content creators, great! If blog content is created by subject-matter experts from different fields or different parts of the organization, perhaps it is possible to invest ownership in one person for all of the blog posts within a specific subject for each field.

If you are in a situation similar to what I described above, where you have multiple, subject-specific owners, it will probably make sense for all of the owners to meet regularly to agree on standards and best-practices for all contributors to follow.

In the end, the fundamental concept here is to place responsibility for all content and every part of a digital property with the people who are in the best position to manage it and ensure its quality, accuracy, pertinence, and value.

Intended Use

Establish the fundamental purpose for the use of each site, application, and tool.

Once we have established ownership for all of the content within our web properties, it may be helpful to define the intended use of those properties next.

This may seem obvious and unnecessary to state, but in my experience it has been important to define the intended use of the web property that is currently being described. This ensures that everyone is on the same page and understands a common set of goals for the property.

Public-facing websites are commonly intended for the use of communicating information to audiences outside of an organization, which is why they are public and usually distinguished from private, inward-facing sites, such as an Intranet, which is intended for the purpose of communicating information to internal audiences within an organization. Not everyone understands this, so it is important to establish the reasoning behind the existence of the property so as not to confuse it with the purpose of another property.

Occasionally, the intended use of a property will be defined in part by the negative, or by that which it is NOT intended to be used. For example, it may be useful to state that no part of a public site should be used for personal content, especially if alternative resources exist explicitly for that purpose.

Here is an example of how intended use is sometimes defined by the negative:

> ***"Academic Department websites are intended for the use of communicating information about the department, its faculty, degree requirements, course offerings, policies, etc. Academic Department websites are not intended for hosting websites of individual faculty, websites based on grant funding, research projects, or specific course-related materials, or for private (i.e. password-protected) websites or applications."***

The negative in this example addresses some misperceptions about the intended use of a site about a department by listing some common misuses of the site previously.

Here are some questions to consider for explaining your own intended use policy:

- What is the primary purpose of the property or website?
- What are the secondary and tertiary purposes, if they exist?
- Are there any activities or content which occasionally find their way onto this property which should live elsewhere, and thus explicitly be listed as not intended for this property?
- What are the "grey areas" or things which are unclear where they belong?
- Is there a process for dealing with grey areas?
- Who would help determine that process if it doesn't exist?

Intended use can be a controversial subject for many organizations, so think carefully and cautiously throughout this exercise. I recommended gathering input from a broad range of representative

stakeholders to discuss some of the stickier points before defining and presenting a plan that may draw criticism when reviewed by the larger organization.

As with most things, intended use should be based in reason and make sense to most people. That being said, there may be occasions in which some level of compromise is required in order to accommodate content that doesn't have a home otherwise. This is typically okay in small amounts and for brief time-periods, until alternative solutions can be found.

Roles and Permissions

Define who should be able to do what in each system.

We live in an era where few institutions have websites and other internet-based properties that are managed and maintained by one or only a few people. Where these spaces were once controlled by the few who knew how to code in HTML, content management systems have now dramatically lowered (and arguably eliminated) the need to possess extensive HTML knowledge. This means that most organizations have lots of people editing their web properties, and without some well-defined rules for all those cooks in the kitchen, things get messy quickly.

Whether or not the platform you are using has roles and permissions built into it, a good governance plan will define roles for users and then apply specific permissions to those roles. Based on my experience, here are some common, fairly generic, roles and permissions that many websites have (or have variations):

- ROLE: Authenticated User
  - PERMISSIONS: Anyone who has activated an account on the website, but has no editing or publishing permissions; authenticated users may be able to see content an un-authenticated user may not see.
- ROLE: Contributor
  - PERMISSIONS: A user with an account who can create new and edit their existing content on the website, but may not publish or delete any content, including their own, or edit content they have not created.
- ROLE: Editor
  - PERMISSIONS: A user with an account who can create new and edit existing content on the website, including content that is not their own; they may or may not publish or delete content.
- ROLE: Publisher
  - PERMISSIONS: A user with an account who can create new, edit existing, publish, and delete any content on the website; typically a person who approves and publishes the work of Contributors and Editors.
- ROLE: Administrator
  - PERMISSIONS: A user with the same permissions as a Publisher, however they may administer accounts, roles, and permissions of other users on the website, along with managing certain site-wide settings.
- ROLE: Webmaster
  - PERMISSIONS: A user with full permissions to all aspects of managing and administering the website, a role typically reserved to the few, most highly trained and experienced users.

These common roles can be modified easily to address the specific needs of your organization.

You may also find that they are lacking certain roles you need, in which case I recommend using one of these for the basis of a new role you create to meet your specific requirements. For example, let's say you have a microsite that is a subset of your main site, and you need to assign a user the role of Administrator ONLY for that micro-site and not the entire main site. Simply take the permissions assigned to

Administrators and create a new role call Micro-Site Admin whose permissions as "Administrator" are limited to only the micro-site that role manages.

Here are some questions to consider to help you begin defining the roles your organization will need, along with the permissions each role should have.

Accounts

- Who should have an account for accessing your website?
- How do users acquire or activate accounts?
- What are the policies for using accounts?
- Is sharing an account permissible?
- What are the conditions under which users may lose their access privileges?

Roles and Permissions

- Who is permitted to edit content on the website?
- Who is permitted to create new content on the website?
- Who is permitted to publish content on the website?
- Who is permitted to delete content on the website?
- Who is permitted to see unpublished content on the website?
- Are there users who should have higher levels of administrative access to perform site-wide changes or to administer user accounts?
- Are there sets of users who need special access to only limited parts or functions within the website?
- Are there limitations to the level of access different users should have?
- Do all users have access to all content?
- Do some users have access to only the content they create?
- Do certain users need to approve content before it is published?
- Does a workflow need to be established for defining how content is produced and published?

Content

Understand how ownership and permissions should apply to content.

In addition to defining ownership for every piece of content on the website, it may also be beneficial to consider and provide guidelines for the many types of content which will appear on the site. Here are some common content types along with some of the questions to consider in defining appropriate usage for your organization.

News and News Listings

- Who is permitted to publish news on the website?
- Which kind of news items are permissible for publishing on the site? Which are not?
- Is there a set of required information that must appear in all news items, such as headline, sub-head, preview text, author name, thumbnail image, etc.?
- How many sources of news or news listings are presented on the site, and what are they?
- Who may publish news to or from these sources?
- Are there editors or gatekeepers who monitor the news that is published or submitted?
- If so, what are the criteria they use for determining which news items are permitted or not permitted?
- What happens to those that are permitted? And to those that aren't?
- May users or groups of user request their own news listing?
- What is the process for acquiring a news listing?
- May the creator of a news item have his or her item appear in the news listings of others?
- What is the process for sharing news with other parts of the site?

Events, Event Listings and Calendars, Event Registration

- Who is permitted to publish an event on the website?
- Which kind of events are permissible for publishing on the site? Which are not?
- Is there a set of required information that must appear in all events, such as title, date, time, location, contact info, thumbnail image, etc.?
- How many sources of events, event listings, or calendars are presented on the site, and what are they?
- Who may publish events to or from these sources?
- Are there editors or gatekeepers who monitor the events that are published or submitted?
- If so, what are the criteria they use for determining which events are permitted or not permitted?
- What happens to those that are permitted? And to those that aren't?
- May users or groups of user request their own events listing or calendar?
- What is the process for acquiring a events listing or calendar?
- May the creator of an event have his or her event appear in the listings or calendars of others? What is the process for sharing events?
- Are events, listings, and calendars hosted by third-party services (such as Google Calendar) permitted?
- May third-party event and calendar content be imported into pages of your website?
- May events have a registration form?
- How is the registration form developed and published?
- Who collects the form submissions, and how is the data collected?

- May payments be collected through the registration form?
- How is the payment collection process managed?

Blogs

- Who is permitted to publish a blog on the website?
- What kinds of blogs are permissible for publishing on the site? Which are not?
- Are group blogs allowed, or are they all individual person blogs?
- Who may publish to or from group blogs? How are bloggers added and removed?
- Are there any rules about the authorship of blogs on the site, such as they must be publicly attributable to the person or group writing them?
- Are there any legal qualifications that need to be addressed for blog content, such as blog content does not reflect the official opinions, policies, or beliefs of the organization as a whole?
- Are there editors or gatekeepers who monitor the blog posts that are published or submitted?
- If so, what are the criteria they use for determining which blog posts are permitted or not permitted?
- What happens to those that are permitted? And to those that aren't?
- May users or groups of user request their own blogs?
- What is the process for acquiring a blog?
- May a blogger have his or her post appear in the blogs of others? What is the process for sharing posts?
- Are blogs hosted by third-party services (such as WordPress or Blogger) permitted?
- May third-party blog content be imported into pages of your website?

Basic or Standard Pages (i.e. general pages of the site, like "About Us")

- Who is permitted to publish basic content pages on the site?
- Once a page is published, who has permission to edit that page?
- Are there any restrictions to the type of content that can appear on a basic page?
- How is the location (within the menu hierarchy of basic pages, i.e. navigation) of new pages determined?
- Do basic pages need to be reviewed or approved prior to being published?
- What are the required elements of a basic page in order for it to be published (i.e. title, sub-title, body copy, preview copy, hero image, thumbnail, URL alias, etc.)?

Images, Audio and Video

- Are images, audio files, and/or videos allowed to be published to the site?
- What file types and sizes are permitted?
- Are there any rules regarding where and how those assets are stored on the site or server?
- Are there any guidelines for how images, audio, and video owned by your organization are to be used on the website?
- May they be edited or altered?
- What types of attributions are required for acknowledging the creator(s) of those assets?
- Do you require release forms from any individuals who may be captured in those assets?
- Do you hire contractors to produce images, audio, or video assets? If so, who owns that material?
- Are images, audio files, and videos hosted on other websites permitted to be displayed on your site?
- Are there any restrictions or limitations to the type, quality, content, authorship, or source of the images, audio files, or videos hosted elsewhere and displayed on your site?
- Are there any guidelines for the use of these types of assets from outside sources.

- What is your policy for using copyrighted material (images, audio, video, as well as textual copy, excerpts, etc.) from outside sources on your website?
- Who is permitted to publish images, audio, and/or video to the website?
- Are there editors or gatekeepers who monitor the images, audio files, and videos that are published or submitted?
- If so, what are the criteria they use for determining which are permitted or not permitted?
- Is there a workflow for the materials that are permitted? And to those that aren't?
- Should users of the site be permitted to download or reuse your copyrighted materials?
- Do you clearly display permission rights on the website?

Embedded Objects and Scripts

- Are embedded objects and scripts permitted to be used on your website, using HTML elements such as embed, script, or iframe?
- Are there limitations to how, when, and where these elements can be used?
- Who is permitted to publish these types of code to the website?
- Are there editors or gatekeepers who monitor the publishing of embedded objects and scripts?
- If so, what are the criteria they use for determining what code is permitted or not permitted?
- What happens to those that are permitted? And to those that aren't?

These are some common types of content and the issues that surround them, but you may have your own set of issues that need to be addressed specifically in your governance plan, so add those wherever it seems appropriate.

Very likely, you have additional content types, beyond those listed above, in your website. You will want to ask the same types of questions as those above about your additional content types as well.

Organization

Establish how the content in your digital properties should be organized and structured.

A website's organization is one of the most important factors in determining how effective and useful the site is for its visitors. Sites that are well-organized, in a manner that visitors intuitively understand, will be more effective and useful than those which aren't. Therefore, it is important to define for your institution who will have the authority and responsibility to determine your website's organization, and how they will make those decisions.

Here are some questions to consider with regard to main websites and subsites within the main site.

Main Website

- Who determines the overall organizational hierarchy of the main website?
- Who determines the top-level menu options? How are those decided?
- Who determines the subsequent levels of navigation, order, labeling, etc.? How are those established?
- Who determines other navigational structures, such as utility menus, topic-based menus, etc.?
- Are there site-wide taxonomies to be maintained? Who determines and edits those?
- What role does usage data, analytics, and user-testing play in those decisions?
- Are there limits to the size, quantity, or depth of navigation?
- Are there any site-wide standards for how navigation and sub-navigation are displayed?
- Is there a process for addressing concerns or proposed changes to the site's organization?
- Who has the ability to make changes to the website's overall structure? Is there are review or approval process that needs to be followed?

Subsites

- Who determines the organizations of sub-sites within the larger website?
- Are there any guidelines or services for website owners who must create their own site organization?
- Are there limits to the size, quantity, or depth of navigation?
- Are there any site-wide standards for how navigation and sub-navigation are displayed?
- Are there any site-wide standards for where navigation and sub-navigation are displayed on sub-site pages?
- Are there rules for the labeling of navigation?
- Are there sub-site specific taxonomies? How are those determined and edited? Must they conform to any site-wide standards or rules?

These questions cover only the definition of responsibility surrounding website organization, which presumes that you have good information architecture in place already. For more information on creating good, test-driven information architecture, Optimal Workshop has both advice and tools for conducting your own card sorts (OptimalSort) and menu "tree" tests (TreeJack). We use these tools regularly in our work.

URL Naming Conventions

Define how URL patterns should be structured in your websites.

A logical progression from website organization is defining a naming convention for URL paths. URL paths should follow a consistent naming convention throughout all of your websites. Only under exceptional circumstances should a URL path name deviate from an established naming convention for a website.

Best practices for URL path naming conventions recommend consistency in how sections, sub-sections, pages, and sub-pages are written. For most websites, I recommend URL paths follow the general naming convention below.

http://domain.com/SECTION/SUB-SECTION/PAGE/SUB-PAGE

This basic structure gives users an idea of where they are in the site's hierarchy of pages. This can be especially important considering the volume of traffic that enters the site from web searches that will bypass the homepage and take visitors directly into deeper pages in the site. It's also a good practice for improving the SEO value of your site's pages, as it provides more specific context for the content of the page.

Section
Under this convention, SECTION is the top-level "directory," and generally refers to the category under which subsequent content resides. For example, in the URL path http://domain.com/about, "About" is a primary category that often appears in a main menu, and thus receives a top-level URL path.

I generally like SECTION names to be one continuous string of letters without hyphens or underscores (e.g. about, services, people, etc.) because that makes for shorter top-level URL paths, however two word hyphens may also be acceptable if they aren't too long. Given that top-level SECTION names are usually the label-names of your main navigation, it's additionally wise to keep them clear, simple and concise.

Acronyms and abbreviations should be avoided because they often don't make sense to visitors unfamiliar with the abbreviations. That being said, some abbreviations, such as http://domain.com/faq, may work so long as they make logical sense to most visitors.

If your website has multiple users who are able to write URL path names, I recommended defining in the governance plan some limitation for who may write top-level directory names. These are typically the most highly sought-after URLs in a website, and you will want to have a well-defined process for how those are distributed and assigned. A free-for-all is probably not a good process.

Sub-Section
SUB-SECTION is the second-level directory, if one exists. Using About as an example, "Meet Our Team" is the second-level "directory" in the URL path:

http://domain.com/about/team

since "Meet Our Team" is just one of the sub-sections under "About" in this example.

SUB-SECTION names also may be one continuous string of letters without hyphens or underscores, such as:

http://domain.com/about/team

or a string of words separated by hyphens:

http://domain.com/about/meet-our-team

The choice between the two really depends on whether the additional words add value to the user's understanding of location, and/or if the string of words adds SEO value because it captures important descriptive words for the content of the page.

In the example above, the words "meet our" really don't add much information, and the shorter URL path name is simpler. Simplicity may become more important as you add pages to sub-sections and the URL path names become very long.

Some URL path names may appear to deviate from this rule if a sub-section does not actually exist, in which case the sub-section location would be occupied by the page name.

Page
Pages on the "Meet Our Team" site would then have a URL path structure of:

http://domain.com/about/team/PAGE-NAME

where PAGE-NAME could be any number of different page names. PAGE-NAMEs should generally describe the content of the page based on the page's title. This can be expressed either as a single word (if a single word sufficiently describes the page), such as:

http://domain.com/about/team/consultants

where "consultants" is a page for information about consultants on the team titled "Consultants"; or by a string of hyphenated words, such as:

http://domain.com/about/team/website-consultants

where "website-consultants" is a page about website consultants on the team titled "Web Consultants."

For the purposes of SEO, at the page level, I generally prefer to include all of the keywords in a page's title (separated by hyphens) in the URL path, especially when it adds descriptive value.

Sub-Page
As follows, sub-pages for any of the pages in the "Meet Our Team" site would have a URL path structure:

http://domain.com/about/team/PAGE-NAME/SUB-PAGE-NAME

SUB-PAGE-NAMEs should follow the same rules as PAGE-NAMEs, however sub-page names may require longer strings of hyphenated names as pages become more detailed and specific:

http://domain.com/about/team/consultants/drupal-content-management-system

Conversely, if sub-pages are breaking out content into simpler categories, they may benefit from shorter names:

http://domain.com/about/services/web-platforms/drupal

rather than:

http://domain.com/about/services/web-platforms/drupal-content-management-system

All of that being said, you should determine the system that works best for your needs and stick to it. Just keep it simple, logical, and as memorable as possible so that it is easy for all users to implement.

Multiple-Word Names
When writing URL paths with multiple-word names, I recommend using hyphens, such as:

http://domain.com/about/services/web-platforms/drupal-content-management-system

rather than underscores:

http://domain.com/about/services/web_platforms/drupal_content_management_system

or concatenation:

http://domain.com/about/services/webplatforms/drupalcontentmanagementsystem

Use of underscores makes it far too easy for a user to misread an underscore as a space, especially when the URL path is hyperlinked:

http://domain.com/about/services/web_platforms/drupal_content_management_system

Most hyperlinks are underlined to indicate to users that a section of text is a hyperlink.

Concatenation is more obviously problematic because it simply creates confusing URL paths.

Aliases and Redirects

How URL path aliases and redirected URL paths are handled will depend on the policies of your organization and the platform you use for your website. I highly recommend you define the rules and processes surrounding URL aliases and redirects in your governance plan, and here are some questions to consider along those lines.

- How are URL aliases and redirects managed in your web environment?
- Who manages URL aliases and redirects?
- Is there a process or procedure for requesting an alias or a redirect?
- May anyone request a URL alias or redirect?
- Are redirects to websites outside of your domain or server environment permitted?
- Who determines whether a URL alias or redirected URL path is appropriate or not?
- Are there any special rules for using top-level directories as URL path aliases or redirected URL paths?

Design

Determine who owns and is responsible for the many aspects design plays in digital communications and properties.

Website design is handled differently by just about every organization I have encountered, but whether you are writing governance for one site with one design or several sites with varying designs and various owners, you will want to document policies and procedures for how sites are designed and redesigned.

For the purposes of this article, I am going to assume we are writing guidelines for a governance plan that must consider multiple sites and site owners. Here follow some questions to consider for writing your guidelines.

General Guidelines for All Websites

- Does your organization have an established visual identity or branding guidelines that will dictate the design of a website?
- Who oversees the adherence to visual guidelines?
- What is the process for having a website design evaluated for adherence to the visual identity or branding? Is there an approval process?
- Are sub-sites within your main website permitted to have their own design, or must they use the same templates designed for the main site?
- What is the process for having a sub-site design evaluated for adherence to the visual identity or branding? Is there an approval process?

Designing New Websites

- Who is responsible for designing new websites? Who is approved or permitted to do this work?
- What is the process for requesting a design for a new site?
- Are there limited design options?
- Are external freelance designers, consultants, and/or design firms permitted to be hired to create a new graphic design for a website?
- Are external freelance designers, consultants, and/or design firms also permitted to produce the templates, themes, or HTML files which constitute the actual execution of the graphic design for the web?
- If external freelance designers, consultants, and/or design firms are permitted to translate the graphic design into files for the web, what formats, languages, protocols, frameworks, and content management applications are permitted in your web environment?
- Are there specific guidelines that external freelance designers, consultants, and/or design firms must be given before starting work?
- Are there dimensional guidelines for the size of the site, such as a maximum or minimum width (or height), or guidelines for breakpoints in responsive designs?
- Are there image-size limits for the purposes of fast page-loading?
- Are there accessibility standards the designs must follow? Must they be tested for accessibility compliance?
- Are there existing style sheets (CSS) that should be used or incorporated?
- Are there specific colors or color palettes that must be used? Or not used?
- Are there specific fonts or font families that must be used? Or not used?

Redesigning Existing Websites

In addition to the questions for new websites, you should also consider the following for redesigning sites.

+ When may a website owner request a redesign of their site?
+ Is there a special process for redesigning a site?
+ Are there any costs associated with a site redesign?
+ May a website owner, or their assignees, make design adjustments to their website between official redesigns, if they have the ability and access to do so?

Personal Websites

Consider the relationship your organization should have with personal websites of members of your organization.

Depending on the type of organization for which you are writing a governance plan, you may need to address the issue of personal websites within the context of your institution's web properties and server environment. For colleges and universities, the questions you need to answer will likely be in relation to faculty, students, and alumni. For businesses, the questions will relate to employees. For non-profits, it may be employees, trustees, and/or volunteers.

Regardless of who the people are, or what function they serve in the organization, if they have a website affiliated with your organization that they control, you probably want to have some guidance for how those properties relate to your organization. Here are some questions to consider for all types of institutions:

- Are there services available for individuals in your organization to have a personal or independent web property (i.e. website, blog, social networking account, etc.)?
- Who provides the service(s)?
- How does an individual acquire the web property?
- Who owns and maintains the web property?
- Where is the web property hosted (i.e. whose servers)?
- Who provides technical support for the web property?
- What levels of support are provided (hosting, domain, programming, training, etc.)?
- Who designs and produces the property?
- Are there guidelines related to visual appearance?
- What happens to the web property if the owner leaves the organization?
- Are there subject matter limitations or guidelines for personal sites?
- Is there any form of review process for content on personal websites?
- What happens if a personal website owner violates subject matter guidelines?
- Who is responsible for costs related to personal web properties?
- Are outside or 3rd-party vendors permitted to work on personal web properties?
- How do 3rd-party vendors access the site and deliver changes?

This list is not an exhaustive checklist for personal website governance planning, but it is a good start that should unearth further questions and circumstances to consider for your plan.

Private Websites, Intranets, and Portals

Determine the policies that should govern sites which are not available to the public.

Most organizations these days have some form of private area for only staff, group members, constituents, partners, vendors, etc. These sites are sometimes guarded behind a firewall and a user authentication system, sometimes just user authentication, and sometimes simply hidden by obscurity. Most often, though, you can identify one of these types of sites because it requires a login and password and is not generally accessible by the public.

Most of the previous questions, regarding content, organization and design are relevant to internal web properties as well, but here are a few questions you may want to ask yourself specifically with regard to private websites, intranets, and internal-facing portals:

- Who owns each one? If they are shared responsibilities, what are the parts and who owns each part?
- How are accounts distributed and access granted?
- Who determines access and account creation?
- What is the process for account creation?
- What is the criteria for gaining access via an account?
- Do user accounts have different roles with different permissions?
- Who are the content editors and creators within the site?
- How is the site edited and maintained?
- Are there any workflows or approval processes for content?
- What distinguishes content that is appropriate for external channels from content that is only appropriate for internal channels?
- Who will be responsible for determining what is appropriate? And how will they enforce those rules?

Public vs Private

Another important consideration for private websites and intranets, especially if you are planning to build one or redevelop your public website, is whether or not an intranet (or a private website) should be a part of your public website. In other words, should the same system for administering and maintaining your public website be the same system as your intranet or private website?

On the surface, the simple answer may appear to be, "Of course! Wouldn't that be the most simple and streamlined approach?" Once you dig into the requirements of what you need for your private site, and compare that with the purpose of your public site, you may determine otherwise.

Why?

The most common purpose for a public website is to communicate information about your organization to a range of audiences, many of whom are not currently part of your organization. In fact, the primary purpose of your public website, specifically, may be to attract those who are not part of your organization in order to convince them to become part of it. In short, your public website's primary purpose is likely to be a marketing tool for expanding your message and growing your constituency (membership, clientele,

user-base, however you think of them). There is not typically a lot of functional interaction that happens between user and website at this stage, aside from asking visitors to contact you, sign-up up for something, attend an event, purchase a product, or some other interaction that is typically managed by a relatively basic form.

In other words, the necessary functionality for a public, marketing website tends to be fairly light in terms of the weight of its programming logic and requirements.

Intranets and private websites tend to be a different animal. Being private, by definition, means they need to support accounts for users. Having a lot of users logging into a system presents a number of challenges and requirements that can become quite complex. A heavier set of tools are often required, adding more software to the system.

Given that users and authentication credentials are involved, often integrations with user databases or user management systems may be involved, and almost certainly, a higher level of security and encryption becomes necessary.

Usually, when you have a private site or intranet, the needs of users become more transactional than consumption marketing information. Once a user is a member, they no longer need to be sold on the organization; they need to "do" things through the website – use tools, access account information, transmit or receive private data, etc. All of these things require deeper levels of programming, security, and the infrastructure to support it – a lot more heft and complexity than what you need for your marketing website, which probably benefits most from being nimble and quick to deliver relevant content.

Perhaps most important, though, is the organization of information – and this is where many projects that aim to combine a public website with a private intranet get bogged down. Since the two sites address the needs of largely different audiences, the menuing and navigation in sites that aim to serve both public and private needs are often in conflict with themselves.

Rarely do you want to show navigation, menuing, or content to the public which is meant only for private users. However, how do you then present the private content and way-finding to authenticated users without breaking a design that, in theory, looks appropriate for only the public content and navigation?

As you get into the details of accommodating both public and private needs on a website, what you often find is that you make odd compromises to things you ordinarily wouldn't (like usability of the site), in order to make the two work together. In truth, given that the audiences for the two sites may have very different needs, and the websites need to serve very different purposes, it is often wise to separate the two, even if that means support two separate systems. In the end, it is better to serve the needs of the users, such that they can be successful using your websites.

Web-Based Applications

Consider use and ownership of web-based tools and applications.

Web-based applications typically add some functionality to your website that it otherwise would not be able to support on its own. These applications tend to come in two varieties:

- those that have been developed internally by your own organization, and
- those that are a service provided to you by a third party (typically a paid service)

Generally speaking, it is likely that internally developed applications are hosted and supported by your organization. When you have an issue, you probably talk to your IT team about it.

Some common internal applications:

- User authentication
- Organizational profiles or staff database system
- Image database system or repository
- Document database system or repository
- Enrollment or student application forms
- Programs and courses database systems
- Products database system

Third party applications are probably accessed via the internet by your website and your users. You (or someone at your organization) probably maintains an account for that service, which you probably pay for monthly or annually. When you have an issue, it is likely someone contacts the third party's support team for help.

Some common third party applications are:

- E-commerce or an online shopping tool
- Donations tool
- Events with RSVP and ticketing
- Appointments, room scheduling
- Live chat

Technically speaking, tools like YouTube, Vimeo, Flickr, etc. are third party application services as well, but they are so easily integrated into your site, often with little or no costs or maintenance, that they require little attention. Still, they may be worth examining when considering governance.

Given the landscape above, your organization likely has several web-based applications – whether those are custom-built applications or third party solutions – which are used to perform specific functions and tasks. Here are some important questions to consider about all of these applications when defining an ownership and governance plan:

- Who owns each application?
- Who is responsible for its technical maintenance and support?
- How are new custom applications developed?
- Is there a process to follow for making functional changes to internally developed applications?
- How is content in the application edited or changed?

- Who is able to change content?
- Who is responsible for maintaining content in the application?
- Is there a process to follow for making content changes?
- How are new third party applications, solutions, or services acquired?
- Who controls the account, if it is a third party application?
- How are third party services expanded or scaled across the organization if needs grow?

There are certainly many more considerations to make based on the specific application or service, and the functionality it offers. I recommend evaluating each application that is a functional part of your website to determine the appropriate governance policies for each.

E-Commerce

Determine the role of e-commerce in your website.

Strict federal laws govern the transmission, collection, and retention of credit and debit card data, whether those interactions occur through the web, by phone, or in person. Any organization involved in collecting payments via credit or debit cards should ensure that all staff involved in a payment collection process are appropriately trained and fluent in the organization's policies regarding the collection and retention of credit and debit card data. And obviously, those policies should adhere to federal and state laws (and international laws, if your reach extends that far).

Minimum Requirements for Collecting Online Payments

Bank Account
Any organization intending to collect credit or debit card payments first needs a bank account in order to receive those payments. The bank account is where the money ***goes*** once a payment transaction is completed.

eMerchant and Payment Gateway
Once you have a bank account where money can be deposited, you will then need to establish accounts with an eMerchant and Payment Gateway provider. Some eMerchant and Payment Gateway services are provided by the same organization. For example, PayPal will handle both the eMerchant and Payment Gateway functions of eCommerce, so all you need to use a service like PayPal is a bank account.

Some organizations have existing payment relationships with companies that serve as eMerchants. It may be more cost-effective to use a company with whom you already have a relationship, in which case there are various Payment Gateway providers that could be used to facilitate the transaction between purchaser and the banks involved in the payment process.

Secure (Encrypted) Online Form
In order to collect the payment details from users, you then will need a secure (meaning encrypted) online form for your website. This is the registration form users will complete with their credit or debit card information to make a payment. The form must be served over a secure and encrypted protocol (i.e. https).

Secure Data Storage
Encryption on the online form is not the last step in security, however. Payment transactions also create customer data, specifically their credit card data, which is highly sensitive and must be handled carefully. Using a reliable payment gateway service eliminates this concern because the entire payment transaction is handled on their secure servers.

Organizations that want to store custom credit card and financial data must undergo a PCI compliance audit and certification. This process is lengthy and expensive, and requires yearly renewals and constant monitoring. We don't recommend doing this yourself, unless the volume of payments are so large that the cost of PCI compliance is less than the fees you will pay a gateway for the service, which is exceedingly rare for the majority of eCommerce websites.

For complex transactions, such as recurring payments, using a reliable gateway service is the only cost-effective option. But even for simple transactions, the general rule is to never store customer payment data. For most organizations, the risks are too high and the costs too great.

Creating a Policy

The minimum requirements for collecting payments online only scratches at the surface of the issues you may need to consider in terms of governing the use of online payment collection for your organization. Here are some additional things to consider:

- Who may have eCommerce capabilities?
- What is the process for initiating eCommerce on the site?
- What is the process for being added to the existing eCommerce solution?
- How many parts of your organization need to collect payments online?
- Do they each need their own implementation of an eCommerce solution? Or can they share?
- Do they each need their own bank account? (This is often the case when reporting of online payments, especially charitable contributions, requires separation between departments or budget lines for accounting purposes.)
- Who is responsible for ensuring that federal and organizational guidelines are followed?
- Where will credit card and user data be saved or stored throughout the payment process?
- Who will have access to any credit card and user data?
- What security practices need to be followed to protect credit card information?

Decisions surrounding eCommerce will invariably involve key decision-makers, stakeholders, and gatekeepers within the Finance department (or correlated function) and IT department within your organization. You are likely to need their cooperation in determining a governance plan for eCommerce.

Broadcast Email

Establish guidelines for the use of broadcast email to constituents and customers.

Broadcast email (i.e. email marketing campaigns, email newsletters, etc.) is loosely defined as email sent and addressed to a group of people rather than a specific person or persons, typically using an email list, contact list, or database of email addresses. It is frequently used for the purposes of email marketing, though it essentially refers to broadcasting a communication to a group of recipients via email to convey information.

When communicating with an external audience, broadcast email typically is sent through an email marketing service (such as MailChimp, Constant Contact, Campaign Monitor, etc.) or through the email platform of a larger enterprise system that may include a CRM and other marketing functions (such as Blackbaud, Salsa, Convio, etc.). Your organization may also have internal mass-email distribution systems in place for broadcast email to internal audiences. For the purposes of this article, we will be speaking mostly about email to external audiences.

Spam

An important issue to address in any broadcast email guidelines is the sending of spam email. Spam email is generally understood to be any email message that is unsolicited and sent in bulk, though whether it is sent in bulk or to an individual is significantly less important than whether the recipients have approved of receiving such emails. This applies to email sent to an address that was not given to the sender explicitly for the purpose of receiving mass email messages from the sender.

Common activities which may qualify as spam:

+ sending a mass email to a list purchased from a company
+ sending a mass email to a list borrowed from another organization
+ sending a mass email to a list compiled by scouring websites for email addresses
+ sending a mass email to a list of recipients to which you have not been given permission to email
+ sending a mass email to a list compiled from a database without permission from the database administrator(s)

Policies

It is critically important to have policies governing broadcast email communication, as it will certainly impact your efficacy in communicating with many of your most important constituencies. Here are many other questions and issues to consider while crafting your governance plan:

+ What broadcast email platforms are available?
+ Who has access?
+ May individuals use their own email accounts (i.e. their personal email account provided by your organization) for broadcast email?
+ Are there multiple lists of broadcast email recipients such as various subscriber lists, audiences, or groups?
+ Who is responsible for maintaining each of these lists?
+ Are permissions and approvals required for sending email to broadcast email lists?
+ Are there any regularly scheduled broadcast emails (such as newsletters)?

- May an individual add information to regularly scheduled broadcast emails?
- May broadcast email recipients unsubscribe from the list(s)?
- Do you have an official unsubscribe policy?
- May members of your organization create and maintain their own custom broadcast email lists?
- What are the guidelines for custom lists?
- Do you have a policy regarding the sending of spam email?
- How does your organization define spam email?

Balancing Internal Needs vs Constituents Needs

The end goal of a good broadcast email governance plan is to balance the organization's need to distribute information with the needs and preferences of your various constituencies. It is certainly a fine balance to strike.

Some good practices include learning more about your constituents preferences and providing them with options for configuring their communication preferences. For example:

- How often do they like to receive emails from you?
- Do they prefer occasional summary-type communications over daily alerts, or vice-versa, or both?
- What topics do they like to hear from you about?
- Do they want to read all of the content in the email itself, or be provided with links to full articles on the website?
- Would they like to be able to change their preferences as their relationship with your organization evolves?

The more you know your audience, the better you can accommodate their needs and minimize the risk that your communications will be perceived as irrelevant, or worse, as spam.

Social Media

Set standards for the establishment and use of social media tools within the organization.

Social media has proven to be an amazingly simple yet powerful digital communications tool. In general, social media tools have a very low barrier to entry. They are easy and intuitive to use, providing a platform for immediate distribution of communications to broad, public audiences. While all of these features of social media are great benefits, they come with obvious risks as well.

By now, we are all familiar with some of the pitfalls and trouble into which users of social media can find themselves. Even very well-intentioned use of social media can lead to embarrassments for individuals and organizations. Once a communication hits the internet and is public, it is nearly impossible to ever fully retract it.

Given that social media accounts are provided and administered by the social media companies themselves, and not your organization, you may not consider all social media accounts to be part of your organization's official digital properties. Regardless, it is sensible to consider policies and guidelines around their use, as it can be a very gray area at times. Here are some questions to consider when crafting such guidelines:

Individual Use

+ Do you need to have a policy around personal use of social media, as it relates to communications that may have an impact on your organization?
+ Are employees allowed to use their personal social media accounts to talk about their work?
+ Are individuals allowed to create and maintain individual social media accounts on behalf of your organization?
+ Are there any approvals required before an employee can create an account on behalf of the organization?
+ Are their guidelines for what is an acceptable use of social media accounts related to your organization for individuals?

Departmental Use

+ Are departments or sub-groups within your organization allowed to have social media accounts?
+ Are their guidelines for what is acceptable use of social media accounts related to your organization for departments and sub-groups?
+ Can social media accounts be shared among employees (i.e. if there is a department social media account, can multiple people use it)?
+ How are credentials for shared social media accounts safeguarded?

Content

+ Do you need content guidelines for users of your social media accounts?
+ Do you need policies for responding to questions or comments provided by other social media users?

- Do you need policies for handling of comments from other users, or content connected to your account from other users, that may be deemed offensive or otherwise problematic for your organization?

Access

- Who should have access for social media accounts that are owned by your organization?
- How is that determined and administered?
- How is access and ownership of social media accounts transitioned in cases of staff turnover?
- How are accounts closed or shutdown if the owner/maintainer of that account can no longer keep it active?

General Questions

- Are there limits to the number of social media accounts that can be created on behalf of your organization?
- Are there restrictions to which social media platforms may be used?

These questions obviously lead to many others, but this is a good start in thinking about the landscape of governance for social media and how it relates to your organization.

Digital Communications Governance

Keep the guidelines you create updated and relevant.

Creating a digital communications governance plan can be a lot of work – probably too much for one person alone – and the decisions that need to be made in crafting its policies, guidelines, and practices are almost certainly not going to be made by one person alone. In most organizations, these decisions are made through consensus by a representative group of stakeholders (or their assignees).

The process for defining, documenting, and enacting such governance decisions requires (at minimum) three components:

+ a team to make decisions
+ a document to capture decisions
+ a process to make changes

Digital Communications Governance Review Board, Committee, or Group

The first component is assembling a team that is representative of the necessary stakeholders, who are empowered to make decisions about governance. We'll call this the Digital Communications Governance Committee, but you can call it anything you like.

The Digital Communications Governance Committee should be an advisory group to help inform policy and governance of the organization's digital communication properties. Ideally it is led by a Chair who is well-informed about digital governance issues at your organization. The group should meet once or twice a quarter to give input on new issues and policies, as well as maintenance of existing policies. And the Committee should have representation from the main administrative areas of the organization, preferably those with knowledge of the modern web and current technologies.

These recommendations are something of a best-case scenario. In other words, it may not be feasible for your organization to convene such a group or meet as often as prescribed. That is fine.

What is important is to have an empowered team who can meet and make decisions when needed.

It's better to do what works for your organization than to try and fail to meet an ideal.

Digital Communications Governance Document

The second component is drafting a document that captures the decisions of the Digital Communications Governance Committee. This document should describe the policies, practices, and procedures that will guide your organization's decisions with regard to governing public digital communications.

Given that circumstances and technologies change rapidly, this should be viewed as a living document in need of regular maintenance and updating to best reflect and address the needs of the organization moving forward. This maintenance explains the need for regular assembly of and discussion within the Digital Communications Governance Committee.

Lastly, the document needs to be shared with and always accessible to the users of the digital communications systems covered by these guidelines. Adherence to the policies and guidelines

diminishes considerably if they are not shared with or readily accessible by the people who need to know them. Changes to policies also need to be communicated explicitly to all who are impacted by the changes. Updating the document itself does not qualify as being clearly communicated.

Digital Communications Governance Amendments
Finally, the third component is a process for making changes to your governance policies. You will need mechanisms for making additions and alterations to your governance plans, as your organization changes, as technology changes, and as circumstances change.

Any issues regarding the policies, practices, or procedures in your Digital Communications Governance Document – or those not considered under your document – should be settled by the Digital Communications Governance Committee, and the results of which should be amended within or added to the document. That makes fairly obvious sense.

You will also need to determine how changes are recommended, how those changes are introduced, debated and decided. Can people outside of the Digital Communications Governance Committee request changes or additions? Along those same lines, there may be instances in which it is beneficial to survey staff on their use of certain tools and properties in order for the Committee to make sound choices.

Digital communications work best when their governance considers the needs of its users balanced with the interests of its primary stakeholders. Open, honest, and respectful dialogue is key to reaching the best outcomes for everyone. Add to that clear ownership, responsibility, and accountability, and your organization will be well on its way to healthy and productive digital communications.

For more content like this from Palantir,
keep an eye on our blog at Palantir.net/ideas.