Date: 03/28/19

Version 1.0

IT Governance Policy Template

# 1. 0 Purpose

IT governance is defined as the processes that ensure an effective and efficient use of IT. It includes processes by which organizations ensure the effective evaluation, selection, prioritization, and funding of competing IT investments; oversees their implementation; and measures business outcomes. Moreover, IT governance is concerned with ensuring that the IT organization (or contractor) operates in an effective, efficient and compliant fashion.

IT governance focuses specifically on information technology systems, their performance, and managing risk. The primary goals of IT governance are to assure that the investments in IT generate business value, and to mitigate the risks that are associated with IT. This can be done by implementing an organizational structure with well-defined roles for the responsibility of information, business processes, applications, and infrastructure.

IT governance ensures processes and conventions are in place to address alignment with your company’s business strategy; to ensure accountability for the management of these systems; to assess performance; to manage risk and to communicate how decisions are made to customers and stakeholders, as well as to your employees.

**2.0 Approach**

The IT Governance Policy Template is intended to assist your company in developing your own IT Governance process. Presented below are the sections that need to be completed in designing your governance system.

**3.0 Board and Leadership Team**

**A. Phase 1 - Building the Framework** - The first phase begins with defining the governance system used by the organization. This IT Governance Policy Template will assist your team by building the framework for a governance system and will prompt you on the sections and issues to consider. The process is composed of three governance practices that:

* evaluate
* direct
* monitor

Your company can model your governance system through the use of this document.

# 2.0 Policy - Personal Accounts

A. Comply with rules and regulations of the site you are using;

B. All pertinent Company information security and privacy policies still apply;

C. Disclose your affiliation with our company

1. Indicate on your profile or blog landing page that “the opinions expressed are my own personal views and not those of my employer”;

D. Do not post on behalf of or attempt to represent our company unless you are authorized to do so;

E. Do not post any internal or confidential information that you obtain or learn about as part of your duties at our company, including but not limited to:

1. intellectual property, personally identifiable information, information technology and security data, business strategy, or other proprietary information;

F. Accurately represent the information and content you are sharing as yours. Accurately credit all sources and respect copyright and intellectual property laws, to include those covering music, videos, text, and images;

G. Assume all information that you share over social media is public, regardless of whether a particular type of content is marked as “private.”

## 3.0 Policy - Company Accounts

A. All accounts must comply with our company’s polices, to include our information security policies;

B. All official accounts must use strong, unique passwords, and where possible must use two-factor authentication (typically a one-time code sent via SMS or generated on a mobile application);

Date: 03/28/19

Version 1.0

IT Governance Policy Template

**B. Phase 2 – Ensure Value Creation -** The second phase is composed of three processes (listed below) which are implemented in parallel, because there are dependencies between them:

1. Ensure benefits delivery - optimize performance and sustainability through the use of IT. Determine which processes can be supported by IT, ensure IT is enabled with bolted in security provisioning);
2. Ensure risk optimization - determine all legal compliance requirements and ensure they are met; and determine how the use of IT can improve the efficacy of audits;
3. Resource optimization - leverage the use of information as a strategic business asset and ensure the implementation of strategies and systems for effective information management and information security.

**C. Phase 3—Stakeholder Management -** The third phase of building a governance system is focused on ensuring stakeholder transparency.

1. Evaluate stakeholder reporting requirements - focuses on collecting the requirements necessary to provide information to stakeholders and customers;
2. Determine stakeholder communication strategies and communicate effectively;
3. Monitor stakeholder communication reporting requirements and solicit feedback on how well you are doing.

**D. Phase 4 - Board and Leadership Approval -** The last phase is to obtain board and leadership approval of the governance plan. Ensure the CEO and/or Board approves the governance system, and signs the IT governance document.

## 4.0 Assumptions and Risk Analysis

A. Risk analysis is the systematic identification of potential areas of uncertainty or concern. In IT, there are many risks such as failed projects, disruption of service, intentional sabotage, poor requirements and inadequate scope definition. These risks could result in costly rework, cost and time overruns, loss of revenues, unhappy customers and unsatisfactory regulatory compliance and controls (e.g. Sarbanes-Oxley, FDA, FCC, and SEC). There are three primary aspects of risk management to be considered:

* risk identification and analysis
* risk quantification and
* risk response, mitigation & contingency plan development.

.

In this section of the document, list the results of your risk analysis and how the company plans to either mitigate the risk, accept the risk, or transfer the risk (such as through an insurance policy). Describe any risks that can occur while implementing a system and the mitigation or remediation strategies for those specific risks. List the assumptions that were included as part of the risk analyses.

## 5.0 Management

## A. Hardware Assets - Provide a list of hardware assets and supporting equipment. Include all hardware used for testing. Ensure the list provides the unit’s specification and date of purchase and any maintenance schedules.

## B. Software Assets - Provide a list of software assets required to sustain the business. Ensure the list provides the version, date of purchase and any maintenance/update/patch schedules.

## C. Services - Provide a list of service agreements. List all hosting agreements, security services and other managed services provided on-premise and off-premise. Include all software that is provided as a service (like O-365). Ensure the list provides the contract duration and terms of use.

**D. Networks -** Describe the network topology and configuration of your network to include on-prem and off-prem. Describe how data moves throughout your business and how it supports a specific business process. Ensure that documentation contains information on how traffic is exchanged through systems and how the internal network is hidden from the outside. Describe how the network is continuously monitored and how company personnel are notified in the event of an intrusion. Cross reference what is stated here in your company’s cybersecurity policy.

**E. Data -** Describe how your organization conducts an annual data inventory. Describe how sensitive data is protected in broad terms. Describe how you comply with GPPR such that you have a data protection officer and how you support a request from a user *“to be forgotten”.* Describe howsensitive data transits over a trusted path and the mechanisms in place to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin. Lastly, describe how you permanently delete sensitive data when no longer needed.

**F. Privacy** - Provide a brief description of the privacy laws and regulations your company has to follow (HIPAA, Privacy Act, Graham-Leach-Bliley, GDPR, etc.). Provide a reference to your company’s privacy policies. Briefly describe your company’s privacy approach or framework. Describe whether there are different laws or regulations that apply to different regions or countries your company operates in. State whether your company has a person in charge of privacy and identify that person by name or by title.

.

IT Governance Policy Template

Date: 03/28/19

Version 1.0

Date: 03/28/19

Version 1.0

Describe whether your company requires a formal Privacy Impact Assessments (PIAs) for systems, and the approach for deciding whether a PIA is required for a system. For systems with PIAs and for company-wide PIAs, and describe where the final PIA reports are located.

Briefly describe the technology protections to safeguard your sensitive data, such as encryption, network access control, user access control, data loss prevention (DLP) systems, etc. Briefly describe what privacy training employees must take.

## G. Authorization and Assessment Process - Establish and document an authorization and assessment process for your company. Describe how new systems and services are introduced to the company to include vetting of the product; who has the decision on purchase; what would be the testing protocols, when approvals are given to move from testing to production; and who approves the final acceptance.

Briefly describe how your company integrates IT security into the IT systems it utilizes and deploys. Include how employees are trained on proper use. Describe how audits are conducted and how the findings are ameliorated and integrated into budgeting and planning processes.

**H. Change Management** - Establish and document your company’s change management process. In this section, document the process to make changes, how recommendations are considered, how the decisions are documented as well as what changes are rejected and the reasons, and the approving authority. Describe how major IT investments are introduced into the business environment. Items to include in the plan:

1. Describe the methodology to implement the change;

2. Describe the testing (both a and b);

3. Describe the approval processes;

4. Describe the steps to implement the new IT and schedule for deployment;

5. Describe the user training;

6. Describe how the system will be sustained over time.

## 6.0 Disaster Planning, COOP Plans

Reference your Company’s Disaster and Recovery Plan. Briefly describe the processes to recover, backup, retrieve and protect your significant data and systems. Include the POC for your company for disaster and/or crisis management.

## 7.0 Implementation Plan

This section should describe guidelines for implementing IT systems for your company.

## 6.0 Disaster Planning, COOP Plans

F. Threat actors may use social media sites for phishing; scrutinize all content on social media as you would email. Use link un-shortening services to avoid being unknowingly redirected to a malicious site;

G. Keep your computing devices’ operating system, browser, and security software up to date.

# 5.0 Applicability

A. This policy applies to both official company accounts and personal accounts of employees and contractors. The policy applies to all contributions to blogs, wikis, social networks, discussion forums, or any other kind of social media.

# 6.0 Other Applicable Policies

A. See our Wi-Fi Policy.

# 7.0 References:

<https://www.scribd.com/document/33461366/Cisco-Social-Media-Policy-Guidelines-and-FAQs>

<http://forums.bestbuy.com/t5/Welcome-News/Best-Buy-Social-Media-Policy/td-p/20492>

<https://www.forbes.com/sites/forbeshumanresourcescouncil/2017/05/25/why-your-business-needs-a-social-media-policy-and-eight-things-it-should-cover/#3e35ef7d5264>

<https://www.coca-colacompany.com/content/dam/journey/us/en/private/fileassets/pdf/2014/01/social-media-principles-english.pdf>

<https://blog.hootsuite.com/social-media-policy-for-employees/>

<https://web.archive.org/web/20170204223204/https:/www.cio.gov/wp-content/uploads/downloads/2013/07/Privacy-Best-Practices-for-Social-Media.pdf>

<https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/social-media/>

IT Governance Policy Template

**A. Schedule** - Describe the schedule of tasks to be completed during the implementation period of a corporate system. Display the tasks in chronological order; that show beginning and ending of each task, the point of contacts for each task, and milestones that will impact the implementation.

**B. Cost** - Describe the way costs will be allocated between tasks/systems/processes that are needed during the implementation period. Also, include the list of accepted risks and false positive risk items based on the risk analysis conducted.

**C. Impact** - Describe the financial benefits and consequences of implementing the system(s). Be sure to provide the business processes associated with the implementation, how it can impact the business and the duration of the process in accordance with the individual steps.

## 8.0 Roles and Responsibilities

## A. Leadership - Define who will approve the IT Governance Plan.

B. **Management** - Define who will maintain the IT Governance plan activities.

**C.** **IT Manager** - Define who is the IT manager for the company and their responsibilities as it relates to the IT Governance Plan.

**D. IT Security/Data Protection Officer** - Define roles and responsibilities.

**E. Others** - Define the roles of employees who have a critical role in accomplishing the plan.

Items to include and consider:

* Define the key activities and end deliverables of the process;
* Resolve unambiguous roles and responsibilities;
* Document each key process’s end deliverables;
* Ensure processes are documented with key activities, procedures and outcomes;
* Ensure roles and responsibilities are formally agreed to upfront and communicated in the form of a matrix of Responsible, Approve, Consult and Inform.

Items to consider in evaluating performance:

* Review individual objectives through regular job performance appraisals;
* Whether roles and responsibilities are executed as defined;
* Whether process-related activities are performed in line with goals and objectives.

F. Threat actors may use social media sites for phishing; scrutinize all content on social media as you would email. Use link un-shortening services to avoid being unknowingly redirected to a malicious site;

G. Keep your computing devices’ operating system, browser, and security software up to date.

# 5.0 Applicability

A. This policy applies to both official company accounts and personal accounts of employees and contractors. The policy applies to all contributions to blogs, wikis, social networks, discussion forums, or any other kind of social media.

# 6.0 Other Applicable Policies

A. See our Wi-Fi Policy.

# 7.0 References:

<https://www.scribd.com/document/33461366/Cisco-Social-Media-Policy-Guidelines-and-FAQs>

<http://forums.bestbuy.com/t5/Welcome-News/Best-Buy-Social-Media-Policy/td-p/20492>

<https://www.forbes.com/sites/forbeshumanresourcescouncil/2017/05/25/why-your-business-needs-a-social-media-policy-and-eight-things-it-should-cover/#3e35ef7d5264>

<https://www.coca-colacompany.com/content/dam/journey/us/en/private/fileassets/pdf/2014/01/social-media-principles-english.pdf>

<https://blog.hootsuite.com/social-media-policy-for-employees/>

<https://web.archive.org/web/20170204223204/https:/www.cio.gov/wp-content/uploads/downloads/2013/07/Privacy-Best-Practices-for-Social-Media.pdf>

<https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/social-media/>

IT Governance Policy Template

Date: 03/28/19

Version 1.0

Date: 03/28/19

Version 1.0

IT Governance Policy Template

## 9.0 Performance/Key Performance Indicators (KPIs)

A. Provide a list of Key Performance Indicators, stating how these metrics will be used to assess company performance. Some of the metrics should be tied directly to the performance of the IT systems. Asses how well the IT systems are in supporting the company’s business goals. The KPIs should define who is responsible for accomplishing the goal, how the measure will be used and the time frame.

## 10.0 References

<http://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1252&context=jitim>

<http://www.wiu.edu/university_technology/other_info/it_strategic_plan_and_governance/pdf/IT_Governance_Framework.pdf>

# 11.0 Applicability

A. Describe the applicability of this policy. Does it include only major IT systems over a specific threshold? If so, explain.

# 12.0 Other Applicable Policies

A. See our Company’s Cybersecurity Policy.

## 13.0 Signature Page - Authorization Approvals

By signing below, you approve this Information Governance Plan and that the information provided above is accurate and current.

Role/ Position Title

Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: MM/DD/YYYY\_

(Signature)

Role/ Position Title

Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: MM/DD/YYYY\_

(Signature)

Role/ Position Title

Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: MM/DD/YYYY\_

(Signature)

Role/ Position Title

Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: MM/DD/YYYY\_

(Signature)

IT Governance Policy Template

Date: 03/28/19

Version 1.0