THE BOARD OF SUPERVISORS OF THE COUNTY OF STANISLAUS
ACTION AGENDA SUMMARY

DEPT: Strategic Business Technology MC

BOARD AGENDA # *B-2

Urgent ☐ Routine ☑

AGENDA DATE October 16, 2012

CEO Concurs with Recommendation YES ☑ NO ☐ (Information Attached)

4/5 Vote Required YES ☐ NO ☑

SUBJECT:

Approval to Accept the Stanislaus County Cloud Computing Policy

STAFF RECOMMENDATIONS:

Approve the Stanislaus County Cloud Computing Policy

FISCAL IMPACT:

There is no fiscal impact associated with the approval of the Stanislaus County Cloud Computing Policy. Vendor compliance will be monitored by existing staff.

BOARD ACTION AS FOLLOWS:

No. 2012-520

On motion of Supervisor Monteith , **Seconded by Supervisor** Withrow
and approved by the following vote,
Ayes: Supervisors: Chiesa, Withrow, Monteith, De Martini and Chairman O'Brien
Noes: Supervisors: None
Excused or Absent: Supervisors: None
Abstaining: Supervisor: None

1) X **Approved as recommended**
2) _____ **Denied**
3) _____ **Approved as amended**
4) _____ **Other:**

MOTION:

Christine Ferraro

ATTEST: CHRISTINE FERRARO TALLMAN, Clerk

File No.

DISCUSSION:

In recent years the term the "cloud" or "cloud computing" has become a regular term in our technology vocabulary. The Internet is sometimes referred to as the "cloud". Cloud computing (also known as "hosted services") is the array of Internet-based services often available to the public and organizations for gathering, storing, processing and sharing information. For the general user who wants a convenient, Internet-based solution for storing or sharing personal information, cloud computing may provide a reasonable option. Examples of such services are Apple's "iCloud" or Google's "Gmail". However, those services evaluated in a business or government context pose additional challenges and need to be analyzed and evaluated against Stanislaus County's security and confidentiality concerns.

While cloud computing services, especially free ones, may offer some level of security and confidentiality, they often do not guarantee that the data you place there will be secure or treated confidentially in order to shield themselves from liability should your data be misused, stolen, or otherwise inappropriately accessed. In most cases, these standard terms and conditions of usage are inappropriate for use with County documents and data. If a County employee is using cloud based services to store, transmit or share County data without Department Head approval, it is a violation of the County IT Security Policy.

As technology advances and new trends emerge that potentially change the way users interact with County documents and data, it is imperative that we enhance our policies or create new ones to help guide staff in their usage and management of County documents and data. Recognizing that the organization's concerns with cloud computing are not completely mitigated by our IT Security Policy and realizing that they are truly a different set of concerns, the IT Security Special Interest Group (SIG) worked collectively with the County IT Steering Committee and the County IT Managers Group to develop a Cloud Computing Policy.

The Cloud Computing Policy was developed over a 5 month period and representatives from the groups mentioned above met regularly to complete this task. All Department Heads were notified of the proposed policy and given the opportunity to provide feedback. As a result, most departments were involved and have worked diligently in the development of this policy. The IT Security SIG meets quarterly and will continue to work with County IT Groups to keep the Cloud Computing Policy up to date and continue to refine our County's implementation of IT security.

Departments will be expected to comply with the Stanislaus County Cloud Computing Policy when seeking any new cloud/Internet based services where county data is stored or processed offsite. Departments will be given a period of 24 months to work with existing vendors who may not currently comply with the Cloud Computing Policy to become compliant.

There may at times be a need for an exception to the Stanislaus County Cloud Computing Policy. It may be that the County is relying on cloud services that were obtained prior to the policy existing and the service does not meet the current minimum security requirements and will be unable to in the 24 month period provided post implementation. It may also be that there is a special need for a particular service that does meet most requirements, but falls short in an area or two. In these types of situations, an informal assessment will need to be completed that weighs any security concerns against the proposed business value of the service. The requesting Department, County Counsel and the County IT Security Manager will make the assessment. County Counsel and the IT Security Manager will need to agree that an exception is warranted and sign-off on the request.

The County IT Security Manager will work with County Departments and County Counsel in the administration of the Cloud Computing Policy. The County IT Security Manager will continue to hold regular IT Security (SIG) meetings as a vehicle for future policy updates and discussion on regular security concerns.

POLICY ISSUES:

The adoption of the Cloud Computing Policy is consistent with the Board's priorities of Efficient Delivery of Public Services and A Safe Community by providing increased security expectations for any vendor providing cloud/Internet based data storage or processing services to Stanislaus County Departments.

STAFFING IMPACTS:

Existing staff from Strategic Business Technology and County Counsel will administer the ongoing policy implementation.

CONTACT PERSON:

Mike Baliel, IT Security Manager, Telephone: 209-342-1737

Stanislaus County Cloud Computing & Hosted Services Policy

Cloud Computing

The Internet is sometimes referred to as the "cloud" and "cloud computing" (also known as "hosted services") is the array of Internet-based services, often available to the public and organizations, for gathering, storing, processing and sharing information. Some cloud services, such as those offered by Apple or Google, may be free to end-users. For the general user who wants a convenient, Internet-based solution for storing or sharing personal information, cloud computing may provide a reasonable option. However, those services evaluated in a business or government context pose additional challenges and need to be analyzed and evaluated against Stanislaus County security and confidentiality concerns.

Dangers

While cloud computing services, especially free ones, may mention computer security and confidentiality standards, they tend not to guarantee that the data you place there will be secure or treated confidentially in order to shield themselves from liability should your data be misused, stolen, or otherwise inappropriately accessed.

Storing County Information

Confidential or otherwise sensitive County information must not be stored, shared, or otherwise processed by a cloud computing service, unless the service/vendor and the County enter into an agreement approved by County Counsel, which includes provisions to protect and manage the data according to standards and procedures acceptable to Stanislaus County. Additionally, the vendor's security compliance will need to be verified by the Stanislaus County Information Security Manager. Security verification needs to be completed prior to establishing any agreements with the County. This applies to cloud services only. This does not apply to products or services that the vendor may offer that are not cloud based. (Note: County employees are prohibited from using personal cloud services without proper authorization, See Stanislaus County IT Security Policy section 8.b)

Service Requirements – Security Verification Matrix

The matrix below should be used to determine if a vendors cloud based service qualifies for County use. To use the matrix, first classify your data as either "Public Access", "Sensitive" or "Highly Sensitive". Departments are responsible for categorizing the data they manage. County Counsel is available to assist with the classification process. Once classified, use the matrix to determine minimum requirements for utilizing a specific cloud based service. Vendors should meet the minimum requirement before pursuing a relationship or agreement.

Requirements	Data Classification		
Description	**Public Access**	**Sensitive**	**Highly Sensitive**
Encryption - At Rest - In Transit	No Encryption	AES 128 / RSA 1024 (or technical equivalent) - Encrypt - Encrypt	AES 256 / RSA 2048 (or technical equivalent) - Encrypt - Encrypt
Data Obfuscation	Not Required	Not Required	Required
Physical Location	Within U.S.	Within U.S.	Within U.S.
Access	All (Read Only)	Assigned Access Secured Access Logged - User ID - IP - Date / Time	Assigned Access Secured Access Logged - User ID - IP - Date / Time
Backgrounds of those who manage the service	Basic Check	Extensive Check - Criminal Record Check (No Criminal Records)	Extensive Check - Criminal Record Check (No Criminal Records)
How is the data destroyed (is there a retention schedule?)	Does not need to be destroyed.	Annual Audit Signed By Company (validating terms of agreement)	Annual Audit Signed By Company (validating terms of agreement)
Security Certifications / External Audits / * SOC 2/3 Reports	No Security Reports Needed	SOC 3 Report or Equivalent	SOC 2 (Type 2) Report or Equivalent
Application Security - Authenticated - SQL Injection Safeguards - XSS Safeguards	- Depends on the need - Required - Required	- Required - Required - Required	- Required - Required - Required
Data Mining/Use Policy	- Allowed	The service will be required to prove that they do not allow 'Data Mining' techniques on customer data. This may be through an opt-out feature for certain customers.	

* See Glossary of Terms

Security Requirements – Other Considerations

Depending on the particular needs of the Department and or the application or service in question, departments may want to look at pre-encrypting data that is going to be stored in a cloud based service. Pre-encryption may take place via secure clients, appliances or other encryption process prior to sending the data to the service in question.

Service Viability

When hosting your data offsite with a 3rd party vendor or in the cloud, you've entrusted the vendor with potentially very valuable information. In some cases, this information may be a critical component necessary to run the business of Stanislaus County. If the data is unavailable or lost, this could put the County at a substantial loss or risk.

Items that need to be evaluated for each vendor:

Fiscal Viability	Each Department will need to determine if their particular need and use of a service is a good fit for the vendor being looked at. For example: If you're looking to host the department's email platform through a vendor, the vendor should be very financially sound with a long track record of doing business (e.g. Google, Microsoft, etc). However, if you're looking to host a small project or program website, then a small local vendor may fit.
Reliability/Failover	Each Department will need to analyze their particular need and use of the service and weigh any concerns against the company's offered "up-time" [Typically, 2 9s (99%),3 9s (99.9%), 4 9s & 5 9s]
Data Recovery	Each Department will need to analyze their particular need and use of the service and weigh any concerns against the company's offered recovery time [Within 2hrs, 4hrs, 8hrs, 24hrs & 48hrs]
Data Portability	How easy is it to migrate from this service at a later date and time? Would you be able to move this service to another vendor or back in house with your necessary data intact? What is the cost to move the data? Has this potential cost been factored into your overall decision?

Exceptions To These Requirements

There may at times be a need for an exception to this policy. It may be that the County is relying on cloud services that were obtained prior to this policy existing and the service does not meet the current minimum security requirements. It may also be that there is a special need for a particular service that does meet most requirements, but falls short in an area or two. In these types of situations, an informal assessment will need to be completed that weighs any security concerns against the proposed business value of the service. The requesting Department, County Counsel and the County IT Security Manager will make the assessment. County Counsel and the IT Security Manager will need to agree that an exception is warranted and sign-off on the request. [See the exception form at the end of this document]

Glossary of Terms

1. **Assigned Access:** Each user accessing the information will have a unique username and password.

2. **Secured Access:** Each unique user will be required to authenticate against a secure service such as an SSL enabled login, SSH or a VPN client enforcing the encryption standards for the given data classification. The service will also need to supply a secure password reset mechanism.

Data Classification Examples

1. **Public Access:** Data/Public Records that are readily and publicly available. For example: Public websites, News Releases, Job Postings, etc.

2. **Sensitive:** Data/Public Records that are only available through a public records request. For example: General County Email Correspondence, County Business Documents, etc.

3. **Highly Sensitive:** Data/Public Records that are protected from public disclosure because of legal privilege. For example: Personnel records, Medical Records, any data restricted by HIPAA, Criminal Records, Documents related to County Legal Matters

AGREEMENT TO

Comply with the Stanislaus County Cloud Computing Policy

This Stanislaus County Cloud Computing Compliance Agreement ("Agreement") is made and entered into by and between the County of Stanislaus, a political subdivision of the State of California (hereinafter referred to as "County"), and _____ (hereinafter referred to as "Vendor"), on _____

TERMS

Vendor hereby agrees to comply with the Stanislaus County Cloud Computing and Hosted Services Policy and Security Verification Matrix for the term of the agreement. Any period of non-compliance during the term of the agreement will be cause for immediate termination of said agreement. Any breach of security or period of non compliance will be reported to the County immediately following the point in time at which the vendor is aware of the breach or period of non compliance. Any failure to report non-compliance or a security breach, will be cause for immediate termination of said agreement.

By: **Vendor (Duly Authorized Representative)**

Name: _____

Title: _____ Date: _____

By: **Stanislaus County, Department:** _____

Name: _____

Title: _____ Date: _____

By: **Stanislaus County IT Security Manager**

Name: _____ Date: _____

Cloud Computing – Security Requirement Exception

REQUEST SECTION

I, _____ (print name) hereby request Security Requirement Exceptions(s) to the Stanislaus County Cloud Computing Policy:

Cloud Computing Service and Company Name:
Security Exception Type(s): Example: (Remove Requirement: Physical Location - US, etc)

Reason(s) for requesting exception(s): (Attach additional pages as necessary)

County IT Security Manager

Name: _____ Date: _____

County Counsel

Name: _____ Date: _____

Attachment to the Stanislaus County Cloud Computing & Hosted Services Policy
Description / Comparison of Service Organization Control (SOC) Reports: SOC 1, SOC 2 and SOC 3

	SOC 1 Reports	SOC 2 Reports	SOC 3 Report
Under what professional standard is the engagement performed?	SSAE No. 16, *Reporting on Controls at a Service Organization* AICPA Guide, *Applying SSAE No. 16, Reporting on Controls at a Service Organization*	AT 101, *Attestation Engagements* AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*	AT 101, *Attestation Engagements* AICPA Technical Practice Aid, *Trust Services Principles, Criteria, and Illustrations*
What is the subject matter of the engagement?	Controls at a service organization relevant to user entities internal control over financial reporting.	Controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy. If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices
What is the purpose of the report?	To provide information to the auditor of a user entity's financial statements about controls at a service organization that may be relevant to a user entity's internal control over financial reporting. It enables the user auditor to perform risk assessment procedures, and if a type 2 report is provided, to assess the risk of material misstatement of financial statement assertions affected by the service organization's processing.	To provide management of a service organization, user entities and other specified parties with information and a CPA's opinion about controls at the service organization that may affect user entities' security, availability, processing integrity, confidentiality or privacy. A type 2 report that addresses the privacy principle, also provides a CPA's opinion about the service organization's compliance with the commitments in its statement of privacy practices	To provide interested parties with a CPA's opinion about controls at the service organization that may affect user entities' security, availability, processing integrity, confidentiality, or privacy. A report that addresses the privacy principle, also provides a CPA's opinion about the service organization's compliance with the commitments in its privacy notice.

	SOC 1 Reports	SOC 2 Reports	SOC 3 Report
What are the components of the report?	A description of the service organization's system. A service auditor's report that contains an opinion on the fairness of the presentation of the description of the service organization's system, the suitability of the design of the controls, and in a type 2 report, the operating effectiveness of the controls. In a type 2 report, a description of the service auditor's tests of the controls and the results of the tests.	A description of the service organization's system. A service auditor's report that contains an opinion on the fairness of the presentation of the description of the service organization's system, the suitability of the design of the controls, and in a type 2 report, the operating effectiveness of the controls. If the report addresses the privacy principle, the service auditor's opinion on whether the service organization complied with the commitments in its statement of privacy practices In a type 2 report, a description of the service auditor's tests of controls and the results of the tests. In a type 2 report that addresses the privacy principle, a description of the service auditor's tests of the service organization's compliance with the commitments in its statement of privacy practices and the results of those tests	A service auditor's report on whether the entity maintained effective controls over its system as it relates to the principle being reported on i.e., security, availability, processing integrity, confidentiality, or privacy, based on the applicable trust services criteria. If the report addresses the privacy principle the service auditor's opinion on whether the service organization complied with the commitments in its statement of privacy practices
Who are the intended users of the report?	Auditor's of the user entity's financial statements, management of the user entities, and management of the service organization.	Parties that are knowledgeable about: • the nature of the service provided by the service organization • how the service organization's system interacts with user entities, subservice organizations, and other parties • internal control and its limitations • the criteria and how controls address those criteria	Anyone