During a meeting between senior executives of your company and potential government customers, you notice that the CEO, CFO, and some of the directors use their tablets and smartphones to access many documents—including those deemed company proprietary—on Google Drive and Dropbox.

Write a policy on the use of cloud-based personal storage space to store company data. The policy must have an overview, scope, definitions, statement of policy, and enforcement.

IN A MS WORD DOCUMENT, ANSWER THE FOLLOWING QUESTIONS (10 points each):

1. The policy will only apply to the offices in the United States.

**User Treaty Advisory Board Meeting**   
   
 – We provide what you require not what you want

**Purpose & Summary:**   
  
The discussion was agenda based with my company and government official of United States of America who is taking are considered to be decision makers for the betterment of the IT organization in USA of uploading and accessing content from cloud storage on what basis does this should happen and whose approval this should takes place. Authoritative position would be taken by the head of the organization taking the context and requirement of the customer. Treating users are not your friends, they should be provided what they want to make the process running rather providing what they want, is the reason which is making us to conduct this meeting, here are some of the inferences/gist and policy information, agreements, decisions we had taken in this meeting. This policy applies for IT firms in USA for making a cloud usage available for users and restrictions over it with its authorization.

**Introduction/Overview:**Policy overview on user utilization cloud storage, restriction and policy adherence made by government officials of United States of America applied on all IT governed related companies in USA for improving the IT enabled security for organization in increasing IT compliance, Integrity and Availability towards the user and trust over the organizations.  
 **Scope:**This policy and all implementing standards and procedures apply to individuals using, accessing, storing, transmitting, or overseeing organization resources, directly or by means of a personally acquired device keeping authorization and approval from higher officials of the organization in constraint. This policy applies to individuals that is owned, operated by IT Companies

or registered under a United States of America IT companies territory. All representatives, contractual workers, advisors, transitory and different laborers at IT Companies in United States of America and its auxiliaries must cling to this approach. This arrangement applies to people that is possessed, worked by IT Companies or, on the other hand enlisted under a United States of America IT organizations region - claimed inside system area.

* CEO, President, Vice presidents, directors, department heads, and heads of centers
* Affiliates, associates, and volunteers
* Third-party vendors, including cases where vendor-owned and/or -managed equipment is housed or used in units

**Definitions:   
  
Affiliates:** All individuals from organizations, stakeholders, external vendors in all means how they are connected, who have been afforded contractual affiliate status by the IT Security of United States of America. Affiliates who receives a check from the IT enabled organizations, Government Organizations for the services they perform.

**Associates:** Individuals such as paid executives, middle level employees, security officials who are having access external group cloud storage who are regularly engaged in activities that directly support the access, uploads, downloads, update to the external cloud storage of IT organization of United States of America.  
  
**Attack:** An attempt to gain unauthorized access or deny authorized access to a external Cloud storage of IT Firms supervisioned by Government of United States of America.

**Availability:** The degree to which information and vital services are accessible for use as on and upon requirement and approved by IT officials supervisioned by Government of United States of America.

**Compromise**: An unauthorized intrusion into an organization resource of United States of America where unauthorized disclosure, modification. or destruction of confidential Organization data may have occurred.

**Confidentiality:** The degree to which confidential Organizational data with external Cloud presence are protected from unauthorized disclosure.

**Device:** Any apparatus used to access, store, transmit, or interface with a organization, personal resource. This includes but is not limited to computers (servers, workstations, and laptops), PDAs, printers, network appliances, devices situated behind firewalls, Network Address Translation devices, or use of Virtual Private Networks also personal drive, personal storage devices, which is mandatory to get registered with the organization Security Department to gain access to personal devices.

**Incident:** An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy (including the Acceptable Use of Computers and Networks policy). The Incident Response Standard team provides several examples of this kind of incidents.

**Integrity:** The degree to which the accuracy and completeness of information and computer software are safeguarded to protect the business process for the IT Firms in United States of America.

**Security Breach:**An unauthorized intrusion into an Organization resource of external cloud storage where unauthorized disclosure, modification, or destruction of confidential Organization data may have occurred.

**Organization Resource:** Data in any form and recorded in any manner, and computer-related resources operated, owned, or leased by the IT Firms supervised by Government of United States of America, including but not limited to

* Networks and network appliances
* Computers (servers, workstations, and laptops)
* Printers
* Software and applications
* Thumb drives, paper, etc.
* Any other computer-related equipment, device, or hardware used to access, store, transmit, or interface with another Organizations resources.

**Volunteer:** An individual, such as a docent, 4-H worker, event coordinator, or other person, who does not meet the criteria for affiliate or associate appointments and is not a IT Firms employees supervisioned by Government of United States of America. Volunteers perform services for the IT Firms without coercion or expectation of compensation, benefits, or future employment.

**Vulnerability Assessment:** An audit by a IT audit department party of Government of United States of America that is intended to identify potential vulnerabilities in a computer system or network.

**Statement:**

Every Individual, employee, stake holders , external vendors who reports to IT Firms in United States of America who adhere to the policy to make a secure and authorized access to external cloud storage access with the approval of Higher officials of Organization and where even it applies to the Subsidiary companies who are directly and indirectly accessing, uploading, downloading or updating the external cloud storage need to approved and authorized by CISO for making an upload, update, access, and download. Approval should also be taken what kind of files can be uploaded to cloud storage from what devices are need to be authorized by CISO of government of United States of America. Each individual, Department, Stakeholders, Subsidiaries, external vendors are been organized to adhere to follow the respective policy to increase security, decrease vulnerability and maintain Complaisance, Integrity, Availability and irresponsibility in implementing this policy in existence, would cause loss of data access privileges, may loss job and may lead to personal civil and criminal liability.

**Enforcement:**

CISO department would review all decisions before approving any kind of decisions taken and it is mandatory all devices of every individual, personal need to get registered to get connected to organization network.   
  
**Copyright Protection**

We respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the U.S. Digital Millennium Copyright Act.

1. Is the general guidance that users should or should not store data on the cloud? Please justify.

Cloud-based platforms house sensitive company data that run the risk of breaches and data leaks. We recommend keeping (encrypted) files and other confidential data stored on your local machine, but recognize the need for knowledge sharing and collaborations within teams. Cloud platforms can also be beneficial when creating backups of files or databases. Please follow the company guidelines outlined before to ensure safe cloud usage:

The use of cloud data storage should be limited to the following platforms: Dropbox and Google Drive to ensure company data is kept safe in a highly encrypted environment. When uploading documents to the Company’s Dropbox and/or Google Drive account, the files will need to be encrypted in transit across a network and at rest. Data must not be accessed through personal smartphones or tablets if they do not have the proper IT security measures put in-place by the IT department. Access to the Dropbox and Google Drive will be limited to the Executive Team and Upper Management. Any employees who do not meet this criteria and need access to these platforms will need to submit an Access Request Form to the Chief Technology Officer for further review.

1. Is there any class of data that must never be stored on personal cloud accounts?

The following class of data should never be stored on personal cloud accounts:

**Restricted or Level 2 Data:** Sensitive documents that contain personally identifying information. These include but is not limited to: financial documents, client-specific documentation, credentials or encrypted passwords. These documents would place the company in great risk if the data was somehow exposed through an attack. Do not upload these documents onto the cloud platforms.

1. Will the enforcement measures be different for senior executives and regular independent contributors (i.e. non-managers)?

Yes, it is different enforcement measures for executive and non-managers. But the first step we should know what duties they are, then can easily answer this question.

1. **GM:**

A general manager of administration is responsible for overseeing all administrative functions in our business. A major part involves leading and directing employees. he delegates administrative tasks, such as accounting, paperwork and payroll, while giving boss the freedom to deal with other issues. In doing so, he ensures administrative efficiency, proper procedure, implementation of policies and employee morale.

**Non-managers employee**:

1, Obey the distribution, follow the command, strictly abide by the operating rules and regulations.

2, Check the operation of the equipment and ensure a safe operation to produce the production.

3 In the production process, if staffs found that the production of quality problems should be promptly processed or reported to MG.

4 Pay attention to improve the ability to innovate, improve the quality of work.

(2)

**1 Manager**

Because the manager is the company's main management staff that can access the company's most confidential information. So it should impose more serious regulations to regulate the operation of the manager. Tablet PC, smartphone as a tool to view the company's top secret is a great potential harm. It even can cause the situation that company can not run.

**2 Non-managers employee:**

For the other employees are almost impossible to access the company's top secret. So there is no need to use and the same way to regulate their behavior.

1. In addition to the policy, research and outline the Terms of Service for two personal cloud storage services, indicating any possible problems these terms of services may bring to the company and to the user, including limited liability, uptime restrictions, etc.

We had researched two personal cloud storage services which are been provided by Google Drive and Oracle Drive, where these are used to upload your files into cloud storage and make it accessible all around the world. Yes, there are some restriction and penalties in the terms of services provided by these two external vendors where there are confirming few points as

#### Liability for Google Drive:

* We will give you prior notice of us suspending or disabling your access to Google Drive. However, we may suspend or disable your access to Google Drive without notice if you are using Google Drive in a manner that could cause us legal liability or disrupt other users’ ability to access and use Google Drive.
* Google and its suppliers and distributors are not responsible or liable for:

(a) losses that were not caused by our breach of these Terms;

(b) any loss or damage that was not, at the time the relevant contract with you was formed, a reasonably foreseeable consequence of Google breaching the Terms; or

(c) losses relating to any business of yours including lost profits, revenues, opportunity or data.

* The total liability of Google, and its suppliers and distributors, for any claims under these terms, including for any implied warranties, is limited to the amount you paid us to use the services (or, if the subject of the claim is the free service, to supplying you the services again).
* Nothing in these terms is intended to exclude or limit the liability of Google and its suppliers and distributors for death or personal injury, fraud, fraudulent misrepresentation or any liability that cannot be excluded by law.

#### Liability for Oracle Drive:

* FORCE MAJEURE: Neither of us shall be responsible for failure or delay of performance if caused by: an act of war, hostility, or sabotage; act of God; pandemic; electrical, internet, or telecommunication outage that is not caused by the obligated party; government restrictions (including the denial or cancelation of any export, import or other license); or other event outside the reasonable control of the obligated party.

References:   
  
1. <http://www.oracle.com/us/corporate/contracts/saas-online-csa-us-1894130.pdf>

2. <https://www.google.com/drive/terms-of-service/>