## Google Drive for WorkGeneral Users/End Users Rules of Behavior

1. Introduction and General System Use

Google Drive for Work is a cloud-based file and data collaboration tool undergoing pilot testing within the Department of Energy (DoE) Entergy Information Technology Services (EITS) environment. During pilot testing, the Google Drive for Work system is authorized to process unclassified, non-sensitive files and data only. There is a disclaimer for web browser access, but not for mobile applications. Users should keep in mind that the same restriction on data usage applies. Files and data stored on Google Drive for Work during pilot testing are not intended to be the primary source files and users should always remember to maintain a primary copy of the file data on their authorized computer.

For the purposes of mobile device usage, only Government Furnished Equipment (GFE), to include GFE phones or tablets, may be used to access Google Drive for Work during pilot testing. Any computer or mobile device should have controlled access implemented in the form of passwords to help prevent unauthorized access to the device. DOE system administrators reserve the right to remotely erase any data on mobile devices in the event a device is reported lost or stolen, user is no longer affiliated with DOE, data spillage, or data contamination.

All data is owned by DOE and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel.  There is no right of privacy in this system, and system personnel may give to law enforcement officials any potential evidence of crime.

Use of this system constitutes consent to this monitoring, interception, recording, reading, copying, or capturing and disclosure.  Finally, all pilot users must agree never to send, store, or post any of the following.

* Classified or Sensitive governmental information
* Official Use Only information
* Close-hold information
* Pre-decisional documents
* Trade secrets, privileged, confidential business, or financial proprietary information
* Personally Identifiable Information (PII), or any information violating the Privacy Act of 1974.
* Source Selection or Procurement Sensitive Information
* Copyrighted materials (without permission)
* Offensive materials, e.g., obscene, defamatory, profane, threatening, harassing, abusive, or hateful.
1. Incident Handling and Reporting

Upon the discovery of a security-related incident, the Google Drive for Work pilot user shall immediately stop work, report the incident(s) (suspected or actual) to their management and contact the helpdesk.

For GFE devices suspected of loss, theft, or compromise, the user/owner must report the incident within one hour and immediately contact the EITS Service center by phone at (301) 903-2500, toll free at (888) 231-5529, or by email at EITS.ServiceDesk@hq.doe.gov. The Network Security Team may also be contacted by phone at (301) 903-3895 or by email at HQNST@hq.doe.gov. Note that a user’s responsibility to report is not complete until acknowledged by DOE. Reportable cybersecurity incidents include the one of the following criteria:

* Actual or suspected storage, upload or posting of unauthorized pilot test data, as defined on the <http://google.energy.gov/>/ web page;
* All suspected and proven attempts for unauthorized access, regardless of whether or not successful;
* Instances of malicious code such as viruses, Trojan horses, or worms;
* Situations involving a person who does not appear to be conducting legitimate business, and is acting in a manner that raises suspicion;
* Instances involving a user who is in violation of these Rules of Behavior, or exhibiting non-compliance with DOE or OCIO policy;
* Actual or suspected loss of media containing Personally Identifiable Information (PII), or the disclosure of PII to unauthorized individuals.
1. Media Contamination and Sanitization
* Should an end user discover that their workstation, mobile device, or network files may have been contaminated due to inadvertent receipt of unauthorized information, the user must immediately cease operation and contact the EITS Service Desk at 301-903-2500.
* If the workstation, mobile device, or other device has been involved in an incident (defined above in section 2 “Incident Handling and Reporting”) or contaminated with classified or other sensitive information, report the pertinent facts and circumstances surrounding a suspected/potential incident to the Energy Information Technology Services (EITS) Service Desk by phone or email at (301) 903-2500, toll free at (888) 231-5529, or by email at EITS.ServiceDesk@hq.doe.gov.
1. Access Controls and Password Management

Google Drive for Work pilot user passwords must contain:

* A minimum of twelve (12) non-blank characters;
* At least one number;
* At least one upper case and at least one lower case non-numeric character;
* At least one special character.

Passwords should not contain the user ID, any common English dictionary word, spelled forward or backwards (except words of three or fewer characters); employ common names; or include the user’s own or, to the best of his/her knowledge close friends—or relatives—names, employee serial number, Social Security number, birth date, phone number, or any recognizable information associated with the user of the password. Passwords should not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx".

Passwords employed by a user during pilot testing should be different than the passwords employed on any sensitive or classified systems.

Passwords should be changed as soon as possible, but within one (1) business day after a password has been compromised, or after one suspects that a password has been compromised; and/or on direction from management.

Individuals must not:

• Connect to the Google Drive for Work pilot testing system from any mobile device other than GFE equipment that has been provisioned for authorized use;

• Share passwords except in emergency circumstances or when there is an overriding operational necessity;

• Leave clear-text passwords in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the password.

1. Acknowledgement

I acknowledge the receipt of, understand my responsibilities and accountability as described by, and will comply with these Rules of Behavior.

|  |  |
| --- | --- |
|  |  |
| Printed Name of Pilot User (Last, First, MI) |
|  |  |
| Date (MM/DD/YYYY) |
|  |  |
| Printed Name of DOE Sponsor (If Pilot User is non-DOE Employee or Contractor) |
|  | Click here to enter text. |
| Date (MM/DD/YYYY) |