The Universities AT SHADY GROVE

Confidential Data Policy
USG Policy 6 (2.00) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

All members of the USG community share in the responsibility for protecting information resources to which they have access. The purpose of this document is to establish minimum standards and guidelines to protect against accidental or intentional damage or loss of data, interruption of USG and Academic Partner business, or the compromise of sensitive information.

This standard applies to all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and all other entities or individuals with access to sensitive information through USG or its affiliates. This also applies to all USG information resources, including those used by the USG under license or contract.

The following industry standards and federal laws help guide the content of this document:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI-DSS)

This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Authentication*: security method used to verify the identity of a user and authorize access to a system or network.

B. *Encryption*: the process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

C. *Mobile Data Device*: a data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

III. Policy Statement

A. All members of the USG community are users of USG's information resources, even if they have no responsibility for managing the resources. Users include students, faculty, staff, contractors, consultants, temporary employees, and guests. Users are responsible for protecting the information resources to which they have access. Their responsibilities cover both computerized and non-computerized information and

information technology devices (e.g. paper, reports, books, film, microfiche, microfilms, recordings, computers, removable storage media, printers, phones, fax machines, etc.) that they use or possess. Users must follow the information security practices set by the OIT Director, as well as any additional departmental or other applicable information security practices.

B. Users are expected to be familiar with and adhere to all USG policies and exercise good judgment in the protection of information resources. They should be familiar with this document and other information-related policies, approved practices, standards, and guidelines, including but not limited to USG's standards regarding acceptable use, access, and privacy.

IV. Physical Security

A. Departments and users must provide physical security for all information technology devices at all times. Physical security should be provided at an appropriate level based on the criticality and sensitivity of data stored and/or processed by the devices. Departments and users should be aware that some data types may require specific physical security controls be in place in order to comply with federal laws and standards.

B. Common physical security controls and practices include but are not limited to:

1. Keeping devices and equipment in locked areas
2. Servers and related equipment are kept in a space protected by at least two factor authentications when feasible. Ensure individuals with physical access is approved and reviewed quarterly (e.g. swipe card plus a numbered code that must be entered to unlock the door).
3. Physical access permissions are reviewed regularly to ensure all faculty and staff with access still have a business need for such access. Reviews should be conducted at least annually for most areas and quarterly for higher security areas such as data centers.
4. Laptops and other portable devices are not left unattended without approved safeguards. (e.g. locked office, secured laptop cabinet, cable locks. etc.).
5. CCTV systems used to monitor entry points for higher security areas such as data centers

V. Access to Information

A. Access to sensitive information should be restricted, electronically and physically, to only persons with a documented business reason for such access. Administrators with the authority to grant access must receive a written request to add users. This request should include the business reason for granting the access along with any details regarding expiration of the access if it is meant to be only temporary. Additionally, users should be required to sign a non-disclosure agreement (NDA) before their access to the sensitive information is granted. Administrators should conduct regular reviews of

system access (at least annually) to ensure all users are still active employees and still require access to the information.

B. If technically feasible, access to sensitive information should be protected through the use of multi-factor authentication (MFA). Additionally, users should connect to systems housing sensitive information using one of USG's secure access services. Finally, user accounts with access to sensitive information should require the use of strong passwords that adhere to the USM IT Security Standards. This may be achieved by linking these accounts to USG's directory services, or another account management system where password complexity can be explicitly defined and enforced.

VI. Information Storage

A. Sensitive information must be kept in a place that provides a high level of protection against unauthorized access and should not be copied or removed from USG.

1. All sensitive information should be stored according to its data classification level; see USG Data Classification Policy 6 (2.10). Information should only ever be stored with data of the same classification level to avoid possible disclosure.
2. Do not store data using sensitive information as identifiers.
3. Encryption consistent with federal and university standards is required for sensitive information stored electronically on all computers; see USG Encryption Policy 6 (2.20). Devices should be encrypted using full disk encryption where technically feasible.
4. Special care should be taken when electing to store sensitive information on any portable devices since these devices are vulnerable to theft and loss.

VII. Distribution and Transmission of Information

A. Sensitive information that is transmitted electronically, transported physically, or spoken in conversation must be appropriately protected from unauthorized interception. For electronic transmissions, utilize encrypted transmission methods; see USG Encryption Policy 6 (2.20). Staff should always connect using one of USG's approved access methods to ensure a secure connection is established.

B. Do not transmit sensitive information via email if possible. If sensitive information must be sent via email, ensure the email can be fully encrypted. Ensure that sensitive information is only ever distributed to persons or institutions with a documented business reason to receive such information. When sensitive information is shared using a shared storage solution (e.g. USG approved cloud-based storage solutions), ensure that those users it is shared with cannot in turn share the information with additional users that should not have access.

C. When sensitive information must be shared with another institution, ensure that it is done so by applying the highest security controls utilized by the two institutions. For

example, if USG requires stricter security than the institution the information is being shared with then USG's security controls should be applied.

VIII. Destruction and Disposal of Information and Devices

A. Sensitive information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. Physical documents containing sensitive information must be shredded prior to disposal. Electronic information should be securely deleted from all locations where stored (i.e. hard drive, network, cloud, etc.) when no longer needed or no longer valid.

B. When hard drives or other devices known to have contained sensitive information reach end-of-life, utilize a secure destruction method to destroy the devices and ensure that information cannot be recovered (i.e. physical destruction of hard drive).

IX. Computer Security Best Practices

System administrators and users should follow a set of computer security best practices to help minimize risk of exposure or loss of sensitive information.

A. Maintain Up-to-Date Software and Firmware
Device operating systems, firmware, and any applications installed on the device should be kept up to date at all times when technically feasible. In general, utilize automatic update functionality wherever technically feasible. If software or firmware cannot be updated automatically then ensure an automatic alert can be generated when a new update is ready for installation.

B. Utilize Virus and Malicious Code Protection
Where technically feasible, install and utilize anti-virus/anti-malware protections. These protections, commonly in the form of software, must be kept up to date at all times. Utilize automatic update functionality to do this.

C. Do Not Leave Device Unlocked When Unattended
Users must either log out or enable a screen lock any time they leave devices unattended. Devices should also make use of an automatic screensaver or screen lock, where technically feasible, that is configured to lock the device after a set period of inactivity.

D. Log out of Applications and Networks When Finished
Some applications are configured to allow users back in automatically without the need to login up to several minutes after the application has been closed. To prevent this, users must log out of their user accounts before closing all applications used to access sensitive information.

E. Configure Automatic Backups for All Sensitive Data
Sensitive information must be backed up regularly to help ensure its availability in the event of a system outage or other adverse event. Backup information should be transmitted to its storage location using an appropriate encryption method; see USG

Encryption Policy 6 (2.20). These backups should be stored in a location that is physically separate from the system from which it originates to protect against loss from natural disaster, fire, or theft. The backup storage location should also employ proper environmental controls necessary to protect the integrity of the backups (e.g. proper HVAC, humidity, and power protections). Periodically, backups should be tested to ensure data is recoverable and that backups are occurring as expected.

F. Configure Automatic Backups for All Sensitive Data
Do not retain sensitive data beyond what is needed. Sensitive information should be deleted/destroyed when no longer needed, no longer valid, or at the end of its retention period; see USG Data Retention Policy 6 (2.30).

X. Incident Handling and Reporting

A. Users must report suspected compromises of information resources, including contamination by computer viruses, to USG's OIT Service Desk (who will inform the OIT Directory and USG Incident Response Team, who in turn will proceed in accordance with the Incident Response Procedure). Incidents must be reported on the same business day users become aware of the compromise.

XI. Security Awareness

A. USG OIT shall provide appropriate security awareness training to all faculty and staff members with access to sensitive information. This training should be provided at the start of employment with USG and its academic partners as well as regularly (at least annually) as a refresher. Training should cover current and common threats as well as appropriate user behaviors.

XII. Accessing Sensitive Information while Traveling

A. Apply the following practices, in addition to all others listed in this document, when accessing sensitive information while traveling:

1. Do not store sensitive information on devices when traveling. Make sure all such information is securely removed from devices before traveling. Sensitive information may be stored within a secure storage solution that is remotely accessible (e.g. approved cloud-based storage solutions).
2. When traveling abroad: Be aware of any applicable export control or other federal regulations that govern the access and storage of sensitive information types from users outside the United States. USG OIT can offer additional assistance. Sensitive information should only be accessed from a trusted computer (e.g. a USG-issued laptop) when traveling.
3. Users should always connect using one of USG's secure access services to ensure a secure connection is established.
4. When connecting to sensitive information, avoid using public Wi-Fi to do so.

5. Clear out cookies and temporary Internet files after each use for all browsers used when accessing sensitive information.

XIII. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

XIV. Revision History

Date	Description	Revised By
06/15/2018	Initial Policy Creation	Russell Schlosburg

XV. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf