Physical Security Policy
USG Policy 6 (1.30) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to protect USG's physical information systems by setting standards for secure and safe operations. This policy applies to the physical security of USG's information systems, including, but not limited to, all USG-owned or USG-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting USG's campus is covered by this policy.

Please note that this policy covers the physical security of USG's Information Technology infrastructure, and does not cover the security of non-OIT items or the topic of employee security. While there will always be overlap, care must be taken to ensure that this policy is consistent with any existing physical security policies.

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as "OIT." 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. *Biometrics*: the process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

B. *Datacenter*: a location used to house a USG's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.

C. *Keycard*: a plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.

D. *Keypad*: a small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.

E. *Mobile Device:* a portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

F. *PDA*: stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

G. *Smartphone*: a mobile telephone that offers additional applications, such as PDA functions and email.

H. *Uninterruptible Power Supplies (UPSs):* a battery system that automatically provides

power to electrical devices during a power outage for a certain period of time. Typically, also contains power surge protection.

III. Security Zones

A. At a minimum, USG will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure USG's assets. In addition to this, USG must provide security in layers by designating different security zones within the building. Security zones should include:

1. *Public*: This includes areas of the building or office that are intended for public access.
    1. Access Restrictions: None
    2. Additional Security Controls: None
    3. Examples: Lobby, common areas of building
2. *Private***:** This includes areas of the building or office that are used only by employees and other persons for official USG business.
    1. Access Restrictions: Only USG personnel and approved/escorted guests
    2. Additional Security Controls: Additional access controls should be used, such as keys, keypads, keycards, or similar devices, ensuring that any physical access controls are auditable
    3. Examples: Hallways, private offices, work areas, conference rooms.
3. *Special Access*: This includes areas that are restricted to use by certain persons within USG, such as executives, scientists, engineers, and IT personnel, for security or safety reasons.
    1. Access Restrictions: Only specifically approved personnel
    2. Additional Security Controls: Additional access controls must be used, such as keys, keypads, keycards, or similar devices, ensuring that any physical access controls are auditable.
    3. Examples: Executive offices, lab space, network room, manufacturing area, financial offices, and storage areas.

IV. Access Controls

Access controls are necessary to restrict entry to USG premises and security zones to only approved persons. There are a several standard ways to do this, which are outlined in this section, along with USG's guidelines for their use.

A. Keys & Keypads

The use of keys and keypads is acceptable, as long as keys cannot be readily duplicated and their distribution is limited. These security mechanisms are the most inexpensive and are the most familiar to users. The disadvantage is that USG has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied and keypad codes can be shared or seen during input. However, used in

conjunction with another security strategy, good security can be obtained with keys and keypads.

B. Keycards & Biometrics
USG requires that keycards or biometrics be used for access to security zones designated as special access areas. USG should consider using these methods for all zones, though it is not required.

V. Physical Data Security

A. Certain physical precautions must be taken to ensure the integrity of USG's data. At a minimum, the following guidelines must be followed:

1. Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information; see USG Confidential Data Policy 6 (2.00).
2. Network ports that are not in use should be disabled.

VI. Physical System Security

In addition to protecting the data on USG's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

A. Minimizing Risk of Loss and Theft
In order to minimize the risk of data loss through loss or theft of USG property, the following guidelines must be followed:

1. Unused systems: If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured.
2. Mobile devices: Special precautions must be taken to prevent loss or theft of mobile devices. Refer to USG's Mobile Device Policy 6 (1.40) for guidance.
3. Systems that store confidential data: Special precautions must be taken to prevent loss or theft of these systems. Refer to USG's Confidential Data Policy 6 (2.00) for guidance.

B. Minimizing Risk of Damage
Systems that store USG data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimize the risk of damage, the following guidelines must be followed:

1. Environmental controls should keep the operating environment of USG systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.
2. Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized.
3. Strong magnets must not be used in proximity to USG systems or media.
4. Except in the case of a fire suppression system, open liquids must not be located above USG systems. Technicians working on or near USG systems should never use the systems as tables for beverages. Beverages must never be

placed where they can be spilled onto USG systems.

5. Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for critical systems and encouraged for all other systems.

VII. Fire Prevention

A. The guidelines below are intended to be specific to USG's information technology assets and should conform to USG's overall fire safety policy.

1. Fire, smoke alarms, and/or suppression systems must be used and must conform to local fire codes and applicable ordinances.
2. Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.
3. Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.
4. Only electrical equipment that has been approved by Underwriters Laboratories or equivalent and bears a seal of approval must be used.
5. Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if possible.
6. A smoke alarm monitoring service must be used that will alert a designated USG employee if an alarm is tripped during non-business hours.

VIII. Entry Security

The guidelines below are intended to be specific to USG's information technology assets and should conform to USG's overall security policy.

A. Use of Identification Badges
Identification (ID) badges are useful to identify authorized persons on USG premises. USG has established the following guidelines for the use of ID badges.

1. USG Employees/Students/Faculty/Academic Partner Staff: ID badges are required.
2. Visitors: Visitor badges are not required, though generic visitor badges are encouraged.

B. Sign-in Requirements
USG does not wish to establish any requirements for employee/visitor sign-in. Use of a visitor sign-in register is encouraged.

C. Visitor Access
Visitors should be given only the level of access to USG premises that is appropriate to the reason for their visit.

IX. 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.

X. Revision History

Date	Description	Revised By
08/22/2018	Initial Policy Creation	Russell Schlosburg

XI. Related Documents

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