Salisbury University

Physical & Environmental Security Policy

1. PURPOSE

The Salisbury University Information Technology (SUIT) department is responsible for, and committed to, managing the confidentiality, integrity, and availability of Salisbury University (SU) networks, systems, and applications within the scope of its authority. To protect the confidentiality and integrity of information technology and data as well as the safety of personnel, agencies must ensure that physical and environmental security controls are established to promote the security posture of the State.

Physical access to information technology processing equipment, media storage areas, and media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

This policy is applicable to all employees, contractors, vendors and agents of Salisbury University. SUIT will be responsible for ensuring adherence to this policy.

4. BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx

- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

5. POLICY

Salisbury University is required to establish physical and environmental controls for critical IT assets under their physical control. Requirements within this policy extend to self-contained facilities such as external data centers, as feasible, and should be considered prior to entering into a contract with an external data center, workplace, or facility. In conjunction with the *Asset Management Policy,* physical and environmental controls must follow the minimum requirements established within this policy.

5.1 Physical and Access Controls

Physical and access controls within the SUIT critical systems will follow the requirements outlined below.

#	Name	Requirement
A	Physical Access Authorizations and Maintenance	Develop and maintain a list of personnel authorized to enter the five SUIT controlled access facilities where information systems reside, and identify those areas in a facility which are designated publicly accessible. These controlled access spaces consist of the following rooms on campus: ◆ WG 103, PH148, HH043, GC003, AC173 Manage the list and all associated logs of access, including: ◆ Track names and status of all who have been issued authorized credentials for facility access ◆ Retain access logs per SU log retention policies where possible. ◆ Regularly audit the detailed access log(s) of facility ◆ Regularly review the access list, and promptly remove individuals from the facility access list when access is no longer required
B	Physical Access Control	Enforce physical access controls for all physical access points to the controlled facilities. This includes: • Verify individual authorization before granting access through the use of picture ID key cards, pin codes, or alarm codes as applicable. • Authorization must be approved by the SUIT manager responsible for the respective secured area. • Control entry to the facility using physical access devices and/or guards • Maintain physical-access audit logs • Provide additional controls where applicable: ◆ Escort visitors at the discretion of SUIT and monitor visitor activity where possible ◆ Secure keys, combinations, and other physical access devices ◆ Inventory who can access physical-access devices regularly ◆ Conduct routine maintenance checks to verify that devices are functioning properly

		◆ Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated ◆ Deactivate or revoke user access credentials upon transfer or termination
C	Access Control for Transmission Medium	Control physical access to system distribution and transmission lines in controlled facilities per the controls listed above.
D	Monitoring Physical Access	Monitor physical access to the controlled facility to detect and respond to physical security incidents, including: ▪ Review physical access logs regularly and upon the occurrence of any known physical-access violation ▪ Report any violations of physical access to critical locations as an incident per the SU Incident Response Policy.
E	Access Records	Maintain visitor-access logs for controlled facilities per the agency retention guidelines, and ensure the logs are reviewed regularly.

5.2 Environmental Controls

Environmental Controls such as power and HVAC required by SUIT Critical systems will follow the requirements outlined below.

#	Name	Requirement
A	Power Equipment and Power Cabling	Protect power equipment and power cabling for information assets from damage and destruction.
B	Emergency Shutoff	▪ Provide the capability to shut off power to information systems in a facility or individual system components in emergency situations ▪ Place shut-off switches or devices in a defined location to facilitate safe and easy access for personnel, while protecting emergency power shutoff capability from unauthorized activation
C	Emergency Power	Provide a short-term uninterruptible power supply (UPS) to utilize if the primary power source fails. Where possible also implement long-term backup power through the use of generators or other alternate power production.
D	Emergency Lighting	▪ Employ and maintain automatic emergency lighting for the information systems that activates in the event of a power outage or disruption where possible. ▪ Lighting should be provided for emergency exits and evacuation routes within the facility.

E	Fire Protection	Employ and maintain **fire suppression** and detection devices or systems for the information systems that are supported by an independent energy source such as UPS. ◆ For the five critical SUIT locations, the following fire controls should be implemented where feasible: • Employ fire detection devices and systems that activate automatically and notify emergency responders • Employ fire suppression devices and systems that activate automatically and notify emergency responders • Employ an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis
F	Temperature and Humidity Controls	Maintain temperature at operational levels within the facility where the information systems reside, and continuously monitor temperature levels. Where possible, humidity should also be monitored and maintained.
G	Water Damage Protection	Protect information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel where possible.
H	Delivery and Removal	Authorize, monitor, and control equipment deliveries, moves, and removals from the facility, and maintain records of those moves.
J	Location of Information Asset Components	Position information system components within the facility to minimize potential damage from **physical and environmental hazards** and to minimize the opportunity for unauthorized access.
K	Regular Testing	Test environmental systems and emergency sources regularly to ensure continuous protections are in place.

6. EXEMPTIONS

If an exemption from this policy is required, an SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted**.**

7. DEFINITIONS

Term	Definition
Fire Suppression Devices	System that uses a combination of dry chemicals and/or wet agents to suppress fires (e.g., fire sprinkler system).
Physical and Environmental Hazards	Flooding, fire, tornadoes, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. May also include location of physical entry points where unauthorized individuals,

	while not being granted access, might nonetheless be in close proximity to information systems.
SUIT Critical System Location	These locations are defined as the following five rooms located at the main Salisbury University Campus: WG 103, PH148, HH043, GC003, AC173

8. ENFORCEMENT

SUIT is responsible for managing security assessments for the University according to established requirements authorized in the SUIT Security Program Policy. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.