De-militarized Zone (DMZ)	(1) Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.
Firewall	A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.
Non-Publicly Accessible Systems	Any system, application, or service accessed by State employees, contractors, vendors, or other authorized entities through an internal, authenticated process restricted to internal network access only, such as logging into a domain authenticated computer.
Publicly Accessible Systems	Any system, application, or service used as a resource by the University and/or constituents of the State of Maryland or external interested.
Remotely Accessible Systems	Any system, application, or service accessed by State employees, contractors, vendors, or other authorized entities from an external connection to any internal resource to administer or to operate an internal resource, such as connections made through VPN.
Secure Sockets Layer (SSL)	A protocol used for protecting private information during transmission via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most Web browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https://" instead of "http://".
Simple Network Management Protocol (SNMP)	An Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
Stateful Inspection	A firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through a firewall. Also known as dynamic packet filtering.
Virtual Private Network (VPN)	A virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

8. ENFORCEMENT

SUIT is responsible for managing boundary control assets for the University. 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.