Salisbury University

Boundary Protection and Internet Access Policy

1. PURPOSE

The establishment of perimeter defense mechanisms is an important part of minimizing exposure to security threats**.** The Salisbury University Information Technology (SUIT) department is committed to managing the confidentiality, integrity, and availability of information technology assets and information. This includes establishing security controls for the boundaries between the University and 3rd party networks including the Internet.

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 networks utilized by the University.

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

SUIT shall establish controls that monitor and manage the flow of information throughout the University network. These controls will govern the flow of information within the internal network (intranet) and at all external boundaries of the information systems and network.

SUIT will oversee management and administration of secure network boundary protection devices (such as routers, switches, **firewalls**, and other boundary protection devices) for the University.

5.1 Boundary Control Devices

SUIT staff shall monitor and control all network boundaries using boundary control devices in a defense-in-depth capacity (e.g. firewalls, routers, proxy servers, etc.). All boundary control devices shall conform to established standards and configurations designated through SUIT configuration management processes. SUIT shall:

- Determine that all points of ingress/egress between network segments in the University or between the University and 3rd party networks including the Internet, are governed by a managed device or combination of devices (such as a firewall and a router) that share boundary control responsibilities
- At a minimum, ensure there are boundary devices that are capable of and configured to perform:
    - Source and destination address filtering
    - Network and port address translation
    - Ingress and Egress filtering to prevent IP spoofing
    - **Stateful inspection**
- Ensure that all firewalls are configured for event logging. Logs must be stored and retained based on SUIT's retention policy, and analyzed daily for malicious/anomalous activities or errors (See *SU Continuous Monitoring Policy*)
- Ensure all IDPS signatures are updated on a regular schedule
- Ensure that all boundary control devices shall be identified and maintained as inventory in accordance with the *SU Asset Management Policy*.

5.2 Publicly Accessible Systems

SUIT shall ensure these systems and services are configured with standardized security controls established and maintained through SUIT configuration management processes (See *SU Configuration Management Policy)*. This process determines the minimum controls needed to protect the confidentiality, integrity, and availability of publicly accessible information, applications, and data.
Publicly Accessible Systems shall not store **confidential information** at rest within the untrusted portions of a network, such as a **DMZ**. All publicly accessible, official websites and systems must use the most comprehensive cryptographic protocol available whenever possible.

5.3 Non-Publicly Accessible Systems

Non-Publicly Accessible Systems must be configured to remain undiscoverable from the public Internet, such as through reconnaissance tactics like ping sweeps, port scans or any other form of discovery, with the exception of the device(s) actually routing and/or firewalling between SUIT and the Internet.

5.4 Limitation of Access Points

The number of ingress/egress points for the University network shall be limited to the minimum number necessary to accomplish the University mission and provide sufficient bandwidth for designated business objectives and contingencies.

5.5 Traffic Flow Rules

All ingress/egress points for the University network shall be governed by Traffic Flow Rules (such as firewall rules and access control lists) that are specific to each point of ingress/egress (or groups of points that abide by the same rules). These Traffic Flow Rules shall be an explicit documentation of each form of network traffic that is allowed through that point. Documented elements for each traffic type will be maintained through the configuration management approved baseline and shall include:

- Authorized protocol
- Authorized sources and destinations
- Authorized TCP/UDP ports if applicable
- Required authentication mechanism, if required
- Business purpose of allowed traffic
- Authorizing individual name and role

5.6 Boundary Control Rule Sets

All devices that contain boundary control mechanisms shall be configured such that:

- All network traffic from an external or untrusted segment shall be denied by default.
- If the device does not include an implicit deny function, then an explicit deny shall be configured in such a way that the same objective is achieved.
- Specific allow rules shall be configured in compliance with the traffic policy for the boundary and shall be written as narrowly as possible to allow only the required traffic.

5.7 Failure of Boundary Protection

In the event of a failure in key boundary protection mechanisms, boundary protection devices will fail CLOSED where this is a configurable option. This ensures connectivity through the devices is disabled and helps to prevent exploitation and loss of monitoring capability. Boundary protection products that only fail OPEN should be avoided where possible.

5.8 Internet Access

Internet access shall be allowed under the following conditions:

- Where possible, all web browsing traffic must be:
  - Compared against blacklists of unauthorized host names, URL elements, HTTP host headers, or other fields relevant to the associated protocol, and dropped if there is a match. Refer to the configuration management documentation for information such as whitelists, blacklists, and URL content filtering.
- All outbound traffic shall be monitored for malicious content;
- All Internet access by employees must conform to the *SU Acceptable Use Policy*.

5.9 Continuous Monitoring

All boundary devices and traffic flow will be subject to the *SU Continuous Monitoring Policy*.

5.10 Management of Boundary Control Devices

Management of boundary control devices should be conducted according to the following mechanisms:

- All SUIT-managed firewalls must be located in secured rooms accessible only to those authorized by management to have access;
- All default administrator credentials shall be changed including SNMP strings (disable SNMP if not used);
- Only SUIT staff authorized to access boundary control devices shall be granted such access; and
- SUIT staff shall not use shared administrative accounts for daily management, but will be granted user-specific accounts.

5.11 Change Controls

Changes applied to boundary control devices or architectures must be approved in accordance with the *SU Configuration Management Policy*.

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**
Confidential Information	Confidential information is considered non-public information and is defined as Personally Identifiable Information (PII), Privileged Information, and Sensitive Information. See *SU Public and Confidential Information Policy.*

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.