Network Blocking Policy

Purpose

Remove threats and enforce compliance with policies on systems connected to BNL networks.

Scope

This policy applies to all BNL computing systems.

Background

Cyber Security maintains the ability to block systems from BNL networks to protect the computing infrastructure from threats and vulnerabilities. This capability is implemented through the core networking equipment with the length of time for a block selected when the block is initiated. Blocks are categorized as **security blocks** and **compliance blocks**. Security blocks are placed when a threat is detected and compliance blocks are placed when a device is not compliant with a policy.

Policy

Cyber Security has the authority to disconnect systems from BNL networks to protect the computing infrastructure from harm (security block) and to force compliance with policies (compliance block).

Cyber Security has the authority to implement a security block on any system at any time based on an observed risk to the infrastructure.

Compliance blocks are implemented within the following time periods:

Identified Vulnerabilities
- High/Medium risk vulnerabilities must be remediated within *seven days* after initial notification to the system owner and administrator.

No Asset Management
- Asset management must be installed within *fifteen days* after the initial notification to system owner and administrator.

Unsupported Operating System
- Operating systems must be upgraded within *thirty days* after the initial notification to the system owner and administrator.

Unregistered Systems
- Visitor network – blocks are placed *forty-eight hours* after detection.
- Internal network – blocks are placed *one hour* after detection.

It is the responsibility of the system owners and administrators to ensure devices are properly registered in order to receive advance notifications of pending blocks.

It is the responsibility of the owners of the compliance blocking processes to provide advance notification to registered system owners and administrators prior to a compliance block taking effect.

In the case of vulnerabilities, it is the responsibility of system owners and administrators to rescan a system to verify the vulnerability has been fixed. A scheduled block is automatically removed when the scan database indicates the vulnerability has been fixed.

In a situation where an automated block cannot be implemented, it is the responsibility of the information system owner to enforce the block according to the above schedules.

The ITD helpdesk is the primary point of contact to reestablish network connectivity.

Major exceptions to the above policy are to be documented in the appropriate information system security plan.

Minor exceptions (short term, individual systems) are handled on a case-by-case basis with Cyber Security.

Revision History

April 12, 2012 – Version 1.06 – Clarified language in the alert process appendix

Appendix – Alert Process

Alert process:

- Alert when detected.
- 2nd alert at the midpoint of the compliance period.
- 3rd alert when the compliance period expires.
- Implement block after short grace period.

When applied for Vulnerabilities:

- Email alert is sent to the system owner and administrator when the vulnerability is detected.
- 2nd email alert is sent out five days after initial notification.
- 3rd email alert is sent out seven days after initial notification.
- A two-hour grace period is then allowed before the block takes effect.

When applied for No Asset Management:

- Email alert is sent to owner/admin upon detection.
- 2nd email alert is sent seven days after initial notification.
- 3rd email alert is sent fifteen days after initial notification.
- A two-hour grace period is then allowed before the block takes effect.

When applied for Unsupported Operating System:

- Email alert is sent to owner/admin upon detection.
- 2nd email alert is sent fifteen days after initial notification.
- 3rd email alert is sent thirty days after initial notification.
- A two-hour grace period is then allowed before the block takes effect.