I. Overview
With the continuing expansion and improvement of the campus *network* and the ever changing technologies involved, it has become increasingly important for the campus IT personnel to work closely together in securely managing the computing and *network* environment. It is in the best interest of the campus *community* to adopt these standards and guidelines for securing local subnet hosts. Doing so will assist in creating a secure *network* environment and protecting the systems within local *units* housed behind the new *firewall* structure.

II. Purpose
These guidelines will assist Net Managers in securing local subnets and working together within the scope of the new *firewall* infrastructure. This document also assists *units* in evaluating how they are meeting the Information Security policies, standards, procedures and guidelines.

III. Scope
This guideline applies to all *devices* connected to the *University network* used to *access*, store, transmit or interface with *University Resources*.

IV. Guidelines
Colleges and Administrative *Units* should create a central IT security group to manage and discuss security issues that affect the *unit*. This would allow for clear communication between colleges/units.

A. *Unit* Level IT Security group:

1) Members should be comprised of *Unit* employees.
2) Create an email list for each Virtual Routing and Forwarding (VRF) context to be used by the security group and managed locally. This list will be added to a campus VRF list for escalation issues.
3) IT Security group tasks:
   a) Determine the main point of contact for questions within the *unit*.
   b) Determine how *firewall* rules may affect others within the VRF.
   c) Determine how to request rule sets within the *unit*.
   d) Assess other security risk(s) within the *unit* as needed.

B. *Unit* risk assessments to determine risks:

1) *Units* must do a self-assessment on *network* subnet devices to determine current threats/risks and create an action plan for remediation for each finding.
2) All devices on the *network* must adhere to the following standards:
   a) Minimum Security for *Networked Devices* Security Standard (IS-S602) and Compliance Checklist
   b) *Server Security Standard (IS-S603)* and Compliance Checklist
   c) Additional risk assessment tools
      (i) *University Network Managers* risk assessment docs *(Action Item)* or ISO risk assessment
C. **Firewalls**
   1) *Firewall* rule changes for campus VRFs must be requested by the subnet manager(s) within the *unit*
      a) Submit request via Remedy ticket
   2) Use the local VRF Listserv for *unit* to share *firewall* rules and request so others will know what is being done (Section 4.A.2 of this document).
   3) Use a *host-based firewall* to protect desktops and internal *servers*
      a) This is required by Information Security Policy/Network Standards (Section 4.b.ii of this document).
      b) Managed and unmanaged systems must, at a minimum, have default OS *firewall* turned on.
   4) If the need for a CPE hardware *firewall* arises, *units* are responsible for installation and management of these devices.  ****

D. **Server Security Scan** Procedure and tools
   1) *Server security scan* request must follow the current scanning standard (IS-P601). This will provide access to the Qualys scanner and setup of automated *scans* of critical *servers*.

E. **Desktop Security Scans** procedures and tools
   1) Net managers should conduct *scans* for desktop vulnerabilities
      a) Create a process/test software/etc… (Action Item)
      b) Secops will use NMAP to periodically scan campus for vulnerabilities and have scan reports available on a quarterly basis from these internal scans.

F. **Incident handling practices.**
   1) Net managers must identify *servers* to UITS for whitelisting against blocking process.
   2) Net Managers must keep contact information up to date via Net Manager database
   3) Reporting
      a) Contact Information Security Office if critical *data* is involved.
      b) Blocking Systems from the *network*:
         (i) Contact UITS to block systems that are infected within *units*
         (ii) Allow current blocking process to block systems as threats are found on the *network*
         (iii) Blocking Criteria:
             a. (see SECOPS document) (Action Item)
         (iv) Admins of whitelisted systems will be contacted via listed contact number. If unavailable for 24 hours, system will be blocked based on judgment call by UITS.
   4) Handling infected/problem systems within a *firewall* context
      a) Requirements to unblock
         (i) Clean up system, document cleanup procedure for verification.
         (ii) ISO or UITS will educate user on incident and how to avoid future incidents
             a. Identify if system is candidate for A/V or *Firewall* software.
   5) Unsupported systems/units recommendations
      a) Recommend contract with WNC for support
      b) Will be placed within general VRF context

G. **UITS** role in **Network Firewalls and Security**
   1) UITS will implement the *firewall* rule requests from netmgrs
2) UITS will setup VRF’s as needed
3) UITS manages device blocking process

H. OPT in/out criteria to move to own VRF or change VRF’s
   1) There may be instances where a *unit* will want or need to have its own VRF. This will be
called for case-by-case review with UITS and ISO to determine if it is in the best interest
of the University’s security posture.
   2) Create a procedure document for review *(Action Item)*

Related Guidance

*Italicized terms* used in this standard are defined in the Information Security Terms Guideline.

**Revision History**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>12/13/2012</td>
</tr>
<tr>
<td>Effective Date</td>
<td></td>
</tr>
<tr>
<td>Revision</td>
<td></td>
</tr>
<tr>
<td>Effective Date</td>
<td></td>
</tr>
</tbody>
</table>