Policy Title: Boundary Protection

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1607 (2014) Boundary Protection

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Boundary protection addresses the measures taken in order to ensure secure communications, both incoming and outgoing, at the physical and digital transition from the University’s information system to the external public networks, or the Internet.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>1</td>
</tr>
<tr>
<td>Stakeholder(s)</td>
<td>1</td>
</tr>
<tr>
<td>Purpose</td>
<td>2</td>
</tr>
<tr>
<td>Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Violations</td>
<td>4</td>
</tr>
<tr>
<td>Interpretation</td>
<td>4</td>
</tr>
<tr>
<td>Publication</td>
<td>4</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>4</td>
</tr>
<tr>
<td>Related Documents</td>
<td>5</td>
</tr>
</tbody>
</table>

CONTACT(S)

Office of Information Technology – (757)823-2869

STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology
PURPOSE

This control is intended to establish the policy and procedures for the boundary protection measures implemented on the University’s information system.

REQUIREMENTS

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and

2. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with a University security architecture.

Supplemental Guidance: Restricting external web traffic only to University web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected sub-network commonly referred to as a demilitarized zone or DMZ). The University considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the University either implements appropriate compensating security controls or explicitly accepts the additional risk.

Control Enhancements for Sensitive Systems:

1. NSU physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces.

   Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

2. The information system prevents public access into the University’s internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

3. NSU limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.
Enhancement Supplemental Guidance: The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.

4. NSU:
   a. Implements a managed interface for each external telecommunication service;
   b. Establishes a traffic flow policy for each managed interface;
   c. Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;
   d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
   e. Reviews exceptions to the traffic flow policy at least once every 60-days; and
   f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

5. The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

6. NSU prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

7. The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

Enhancement Supplemental Guidance: This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent split-tunneling. Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunneling would be, in effect, allowing unauthorized external connections into the system.

8. The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.
Enhancement Supplemental Guidance: A host-based boundary protection mechanism is, for example, a host-based firewall. Host-based boundary protection mechanisms are employed on mobile devices, such as notebook/laptop computers, and other types of mobile devices where such boundary protection mechanisms are available.

VIOLATIONS

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

INTERPRETATION

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;
2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;
3. Post the policy on the appropriate SharePoint Site and/or Website; and
4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:
- Supersedes (previous policy): OIT 62.8.1607 Boundary Protection
RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard