Policy Title: Emergency Shutoff

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1110(2014) Emergency Shutoff

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

A means for the disruption of power to the University’s information system is necessary in the event an applicable emergency situation arises.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th></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>2</td>
</tr>
<tr>
<td>Interpretation</td>
<td>2</td>
</tr>
<tr>
<td>Publication</td>
<td>2</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>3</td>
</tr>
<tr>
<td>Related Documents</td>
<td>3</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 emergency shutoff of the University’s information system and the necessary associated devices.

REQUIREMENTS

NSU:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;

2. Places emergency shutoff switches or devices in University-defined location by information system or system component to facilitate safe and easy access for personnel; and

3. Protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

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 62.8.1110 Emergency Shutoff

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard