Policy Title: Flaw Remediation

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1702 (2014) Flaw Remediation

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Flaw Remediation addresses the intrinsic faults and weaknesses in software and establishes the necessary measures that should be taken to mitigate the risk of exploitation within the University’s information system.

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>2</td>
</tr>
<tr>
<td>Interpretation</td>
<td>3</td>
</tr>
<tr>
<td>Publication</td>
<td>3</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 policy is intended to establish the policy and procedures for flaw remediation on the University’s information system.

REQUIREMENTS

NSU:

1. Identifies, reports, and corrects information system flaws;

2. Tests software updates related to flaw remediation for effectiveness and potential side effects on University information systems before installation; and

3. Incorporates flaw remediation into the University configuration management process.

4. Applies all software publisher security updates to the associated software products.

5. Applies all security updates as soon as possible after appropriate testing, not to exceed 90 days for implementation.

6. Prohibits the use of software products that the software publisher has designated as End-of-Life/End-of-Support (i.e. software publisher no longer provides security patches for the software product).

Supplemental Guidance: The University identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated University officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The University (including any contractor to the University) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. It is encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in University information systems. By requiring that flaw remediation be incorporated into the University configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US Special CERT guidance and Information Assurance Vulnerability Alerts have been accomplished.

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 62.8.1702 Flaw Remediation

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard