Policy Title: Authenticator Feedback

Policy Type: Administrative


Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Authenticator feedback requires management to mitigate the risk of possible exploitation by unauthorized users or systems.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Contacts</th>
<th>Stakeholder(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Requirements</td>
</tr>
<tr>
<td>Interpretation</td>
<td>Violations</td>
</tr>
<tr>
<td>Publication</td>
<td>Review Schedule</td>
</tr>
<tr>
<td>Related Documents</td>
<td></td>
</tr>
</tbody>
</table>

PAGE NUMBER

1  1  2  2  2  2  3  3

CONTACT(S)

Office of Information Technology – (757)823-2869

STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology
PURPOSE

This control establishes the policy for maintaining and managing authenticator feedback within the University’s information system.

REQUIREMENTS

The University information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.

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 62.8.706 Authenticator Feedback

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard