
**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

Threat Management: *Incident Handling*

Incident Response Plan

Strategies Evaluation form

Form ID Number: _____ *(IT Staff use only)*

1. Process ID: (if applicable) _____

2. Date Tested: _____

3. Tested By Team(s): Incident Response Team _____

4. Testing Method: Table Top: _____ Functional: _____ Full Scale: _____

5. Testing Scenario or Incident Details: _____

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

Threat Management: *Incident Handling*

Incident Response Plan

Strategies Evaluation form

a. Assumptions: _____

6. Mitigation Strategy: _____

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

Threat Management: *Incident Handling*

Incident Response Plan

Strategies Evaluation form

7. Was the Mitigation Strategy successful?

a. Yes: _____

b. No: _____ Explain:

Explanation: _____

8. Were written guidelines accessible to the Incident response team?

a. Yes: _____

b. No: _____ Explain:

Explanation: _____

9. Did the team follow procedures and perform appropriately?

a. Yes: _____

b. No: _____ Explain:

Explanation: _____

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

Threat Management: *Incident Handling*

Incident Response Plan

Strategies Evaluation form

10. Was any additional information required, if so what? _____

11. Were there any factors that inhibited the recovery, if so identify them: _____

12. What additional resources are needed to assist in future incidents?

13. Evaluation, Lessons Learned: _____

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

Threat Management: *Incident Handling*

Incident Response Plan

Strategies Evaluation form

14. Reviewed By: SVCC Incident Response Team

15. Date Reviewed: _____

16. Recommendation:

a. Approve Incident Response Plan as stated above: _____

b. Make the following changes: _____
