# C4 3.6: Incident Response

Created by Purdue University NSF # 1840043

| 800-171 Rev. 1 Mapping | Control Family | Required Control | Implementation | Program/Policy/Procedure Reference | Control Gaps |
|---|---|---|---|---|---|
| 3.6.1 | C4.3.6.1 | An incident handling response will be documented, including process and procedure, preparation, detection, analysis, containment, recovery, and user response. Consult with central security services and local IT to develop incident response documentation. Review documentation annually. | ☐Implemented<br>☐Planned to be Implemented (see: Control Gaps)<br><br>**Description:** | | |
| 3.6.2 | C4.3.6.2 | Report all incidents to central security organization, which will centrally track, document, and report incidents. Locally track and document incident response as | ☐Implemented<br>☐Planned to be Implemented (see: Control Gaps)<br><br>**Description:** | Incident Response Policy (VII.B.3) and STEAM Incident Response Handbook | Does RCAC have access to the STEAM Handbook ? |

| | | | | | |
|---|---|---|---|---|---|
| | | instructed by central security organization. | | | |
| 3.6.3 | C4.3.6.3 | Test incident response plan no less than annually via tabletop or similar exercise. | ☐Implemented<br>☐Planned to be Implemented (see: Control Gaps)<br><br>**Description:** | Incident Response Policy (VII.B.3) and STEAM Incident Response Handbook | Does RCAC have access to the STEAM Handbook ? |