Security Operations Center
Operations Manual

08/02/2018

Table of Contents

1 1.a. Process Flows
5 1.b.i. Monitoring - Data Collection
6 1.b.ii. Data Normalization
11 1.c.i Assignment of Roles in an Event
13 1.c.ii. Containment / Collection
14 1.c.iii. Notification Process
16 1.c.iv. Verification and Recovery Steps
26 1.c.v. Postmortem Analysis
32 1.d Member Security Staff Roles and Responsibilities
34 1.e. SOC Hours of Operation
35 1.f.i. After Hours Procedures
36 1.f.ii. After Hours Escalation
38 1.f.iii. After Hours Communications
39 1.g.i. Communication Standards - Members
40 1.g.ii. Communication Standards - Executives
42 1.g.iii. Communication Standards - Law Enforcement
44 1.g.iv. Communication Standards - The Public and the Press
45 1.g.v. Communication Standards - Information Sharing
46 1.h.i. Security Incident Handling Workflow
47 1.h.ii. Procedures detailed overview
49 1.h.iii. Incident Procedures by Type
56 1.i. Reporting & Analysis
57 1.j. Tools-based Procedures
59 2. Contingency / Disaster Recovery
61 3. Network Security
64 4. Physical Security
79 5. Training

I wrote this for the Texas A&M System Security Operations Center. This SOC supports 27 member institutions (campuses and agencies) located all over Texas, with over 180,000 users. Naturally, the details must be confidential.