



Incident Response Standard Operating Procedure

NIC Indiana Network Operations

Abstract

Addresses how to respond to incidents that compromise the confidentiality, integrity, or availability of systems in the NIC Indiana Network

Indiana Interactive LLC Response to RFP 20-1351

PROPRIETARY & CONFIDENTIAL

Kate Congdon
Kate.Congdon@egov.com

PROPRIETARY & CONFIDENTIAL

Table of Contents

1. Incident Response SOP	1
1.1 Overview	1
1.2 Scope	1
1.3 Review	1
2. Incident Response Definitions.....	1
3. Incident Response Personnel.....	2
3.1 Local Incident Response Team	2
4. Incident Response Phases.....	3
4.1 Preparation.....	3
4.1.1 Documentation	3
4.1.2 Toolkit	3
4.2 Identification / Detection.....	4
4.2.1 Via Automation	4
4.2.2 Via Observation.....	4
4.2.3 Initial Response	4
4.2.4 Reporting Time-Frames.....	4
4.3 Tracking.....	6
4.4 Containment	7
4.5 Eradication.....	7
4.6 Recovery.....	8
4.7 Follow-Up	8
5. Incident Response Testing.....	8
6. Incident Response Training.....	8
7. References	8
SECURITY INCIDENT REPORT	10
Appendix A Incident Playbook	12
A.1 Unauthorized Network Access.....	12
A.1.1 Preparation	12
A.1.2 Identification and Detection.....	12
A.1.3 Containment.....	12
A.1.4 Eradication	12

DRAFT

A.1.5	Recovery	12
A.2	Unauthorized Windows System Access.....	12
A.2.1	Preparation	12
A.2.2	Identification and Detection.....	12
A.2.3	Containment.....	13
A.2.4	Eradication	13
A.2.5	Recovery	13
A.3	Unauthorized Linux System Access	14
A.3.1	Preparation	14
A.3.2	Identification and Detection.....	14
A.3.3	Containment.....	15
A.3.4	Eradication	15
A.3.5	Recovery	15
A.4	Unauthorized Apple OS Access.....	15
A.4.1	Preparation	15
A.4.2	Identification and Detection.....	15
A.4.3	Containment.....	16
A.4.4	Eradication	16
A.4.5	Recovery	16
A.5	Distributed Denial of Service.....	16
A.5.1	Preparation	16
A.5.2	Identification and Detection.....	16
A.5.3	Containment.....	16
A.5.4	Eradication	16
A.5.5	Recovery	17
A.6	Malicious Code	17
A.6.1	Preparation	17
A.6.2	Identification and Detection.....	17
A.6.3	Containment.....	17
A.6.4	Eradication	17
A.6.5	Recovery	17
A.7	Improper Usage.....	17

DRAFT

A.7.1	Preparation	17
A.7.2	Identification and Detection.....	17
A.7.3	Containment.....	17
A.7.4	Eradication	18
A.7.5	Recovery	18
A.8	Web Site Defacement.....	18
A.8.1	Preparation	18
A.9	References.....	18

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT