**Name of Organization**

**Incident Notification Form**

**Short**

Nov 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
| DRAFT | 10/21/2021 | Draft version Created | Stealth Group |
| Final | 11/12/2021 | Final Review | Deckwerth |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| Incident Notification Report | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Contact Information | | | | | | | | | | | |
| Name: | |  | | | | Title: | |  | | | |
| Agency/Department: | |  | | | | Email: | |  | | | |
| Office Phone: | |  | | | | Mobile Phone: | |  | | | |
| Incident Location | | | | | | | | | | | |
| Local Contact Name: | |  | | | | Title/Role: | |  | | | |
| Office Phone: | |  | | | | Mobile Phone: | |  | | | |
| Email: | |  | | | | | | | | | |
| Location / Address: | |  | | | | | | | | | |
| Incident Detection | | | | | | | | | | | |
| * Device Alert | | | | * Log Analysis | | * Help Desk | | | | | |
| * End User Alert | | | | * Endpoint Security Software Alert | | | * Law Enforcement | | | | |
| * Other | | | | | | | | | | | |
| Incident Type | | | | | | | | | | | |
| * Exercise / Network Defense | | | | * Denial of Service | | * Improper Usage | | | | | * Investigation |
| * Unauthorized Access | | | | * Malicious Code | | * Scans / Probes / Attempted Access | | | | | |
| * Other | | | | | | | | | | | |
| Incident Characteristics | | | | | | | | | | | |
| Source IP/Port: |  | | | | | Destination IP/Port: | | | |  | |
| Scope of Impact: |  | | | | | Additional Information: | | | |  | |
| Incident Timeline | | | | | | | | | | | |
| Duration of Attack (From): | | |  | | | Duration of Attack (To): | | | | |  |
| Incident Impact | | | | | | | | | | | |
| * Number of Affected Users: | | | | | | | | | | | |
| * System Down Time: | | | | | | | | | | | |
| * System Damage: | | | | | | | | | | | |
| * Service / Information Integrity Damage: | | | | | | | | | | | |
| * Financial Loss: | | | | | | | | | | | |
| * Data Loss / Compromise: | | | | | | | | | | | |
| * Other | | | | | | | | | | | |
| Incident Severity | | | | | | | | | | | |
| * High | | | * Medium | | * Low | | | | * Unknown | | |
| Affected Data Sensitivity | | | | | | | | | | | |
| * High | | | * Medium | | * Low | | | | * Unknown | | |
| Confidentiality | | | | | | | | | | | |
| * Do Not Share – Information may not be shared beyond Enterprise Information Security Officer (EISO) and may be shared with law enforcement if necessary. | | | | | | | | | | | |
| * Share Restricted - Information cleansed of identifying characteristics may be shared with other Security Engineers (SEs), states and other appropriate organizations | | | | | | | | | | | |
| * Share Unrestricted – Information including identifying characteristics may be shared with other SEs, states and other appropriate organizations | | | | | | | | | | | |
| What immediate assistance can the Cyber Command Center offer? | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Additional Notes | | | | | | | | | | | |
|  | | | | | | | | | | | |