

# MSU Information Systems | Incident Response Check Sheet

---

Please complete the following list to the best of your availability to aid Information Systems personnel.

## 1. General Information

1.1 Incident Number: \_\_\_\_\_

### 1.2 Reporting Site Information

1.2.1 Date/Time of Report \_\_\_\_\_

1.2.2 Name \_\_\_\_\_

1.2.3 Department Name \_\_\_\_\_

1.2.4 Title \_\_\_\_\_

1.2.5 Telephone Number \_\_\_\_\_

1.2.6 Fax Number \_\_\_\_\_

1.2.7 E-mail Address \_\_\_\_\_

1.2.8 Office Address \_\_\_\_\_

1.2.9 Domain Name \_\_\_\_\_

1.2.10 Other Contact Info \_\_\_\_\_

## 2.0 Incident Information

### 2.1 System Information

2.1.2 Physical Location of system(s) \_\_\_\_\_

\_\_\_\_\_

2.1.3 Type of device \_\_\_\_\_

\_\_\_\_\_

2.1.4 Machine name \_\_\_\_\_

\_\_\_\_\_

2.1.5 Purpose of system(s) \_\_\_\_\_

\_\_\_\_\_

# MSU Information Systems | Incident Response Check Sheet

---

2.1.6 Current Status \_\_\_\_\_  
\_\_\_\_\_

2.1.7 Operating system(s) of device(s) \_\_\_\_\_  
\_\_\_\_\_

2.1.8 Security in place (i.e., Firewall) \_\_\_\_\_  
\_\_\_\_\_

2.1.9 Can you provide logs? \_\_\_\_\_  
\_\_\_\_\_

## 2.2 Intrusion/Attack Information

2.2.1 Date/Time of Incident? \_\_\_\_\_  
\_\_\_\_\_

2.2.2 Duration of Incident? \_\_\_\_\_  
\_\_\_\_\_

2.2.3 Nature of Problem? \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

2.2.4 Attack Type (i.e., Trojan)? \_\_\_\_\_  
\_\_\_\_\_

2.2.5 Extent of compromise? \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

2.2.6 Damage or loss of information? \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

# MSU Information Systems | Incident Response Check Sheet

---

2.2.7 Source address of the attack? (IP, MAC, etc.) \_\_\_\_\_

## 3. Other Information

3.1 What actions or technical measures have been taken?

---

---

---

3.2 Have you notified law enforcement or another agency?

---

---

---

3.3 If known, please list stakeholders of the compromised system.

---

---

---