IRIS Incident Response Procedure

v1 2021-02-09

1. **(Suspected) Discovery**
    1. ☐ Local Security Team — *If applicable: INFORM* ***WITHIN 4 HOURS***
    2. ☐ IRIS Security Team — *INFORM via security@iris.ac.uk* ***WITHIN 4 HOURS***

    FOR GRIDPP ONLY
    3. ☐ EGI CSIRT Security Team — *INFORM via abuse@egi.eu* ***WITHIN 4 HOURS***
2. **Containment**
    1. ☐ Affected Hosts If feasible: — *ISOLATE* ***WITHIN 1 DAY***
    2. ☐ Affected VMs — *SNAPSHOT and/or SUSPEND* ***WITHIN 4 HOURS***
    3. ☐ Affected Appliances — *DISABLE* ***WITHIN 4 HOURS***
3. **Confirmation**
    1. ☐ Incident — *CONFIRM WITH COORDINATING SECURITY TEAMS*
4. **Downtime Announcement**
    1. ☐ Service Downtime — If applicable: ANNOUNCE WITH REASON "SECURITY OPERATIONS IN PROGRESS" **WITHIN 1 DAY**
5. **Analysis**
    1. ☐ Evidence — COLLECT AS APPROPRIATE
    2. ☐ Incident Analysis — PERFORM AS APPROPRIATE
    3. ☐ Requests from security teams — FOLLOW-UP **WITHIN 4 HOURS**
6. **Debriefing**
    1. ☐ Post-Mortem Incident Report — PREPARE AND SUBMIT **WITHIN 1 MONTH**
7. **Normal Service Restoration**
    1. ☐ Normal Service Operation — RESTORE PER SERVICE PROVIDER **AFTER INCIDENT HANDLING IS COMPLETE**

Based on working hours: 1 day is 1 working day, 1 hour is 1 working hour

REFERENCES

https://www.iris.ac.uk/security