

# EGI Incident Response Procedure — Resource Centre Checklist

Revision 1745 (2015-11-09)

## 1 – (Suspected) Discovery

1. Local Security Team ————— *If applicable: INFORM **WITHIN 4 HOURS.***
2. NGI Security Officer ————— *INFORM **WITHIN 4 HOURS.***
3. EGI CSIRT Duty Contact ————— *INFORM via “abuse@egi.eu” **WITHIN 4 HOURS.***

## 2 – Containment

1. Affected Hosts ————— *If feasible: ISOLATE as soon as possible **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 YOUR LOCAL SECURITY TEAM AND/OR EGI CSIRT.*

## 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 EGI CSIRT ————— *FOLLOW UP **WITHIN 4 HOURS.***

## 6 – Debriefing

1. Post-Mortem Incident Report ————— *PREPARE AND SEND to “abuse@egi.eu”  
**WITHIN 1 MONTH.***

## 7 – Normal Operation Restoration

1. Normal Service Operation ————— *RESTORE AS PER RESOURCE CENTRE STANDARDS  
**AFTER INCIDENT HANDLING IS COMPLETE.***
2. Procedures and Documentation ————— *UPDATE as appropriate to reflect analysis results.*

## References

- EGI Incident Response Procedure ————— <https://wiki.egi.eu/wiki/SEC03>
- EGI CSIRT Wiki ————— [https://wiki.egi.eu/wiki/EGI\\_CSIRT:Main\\_Page](https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page)
- EGI Security Team Contacts ————— [https://wiki.egi.eu/wiki/EGI\\_CSIRT:Contacts](https://wiki.egi.eu/wiki/EGI_CSIRT:Contacts)
- EGI CSIRT Abuse Report E-Mail Address ————— [abuse@egi.eu](mailto:abuse@egi.eu)