EGI Incident Response Procedure — Site Checklist

Revision 1566 (2011-01-05)

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 possible and feasible: ISOLATE AS SOON AS POSSIBLE* ***WITHIN ONE WORKING DAY***.

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 ONE WORKING DAY***.

5 — Analysis

1. Evidence ——— *COLLECT AS APPROPRIATE*.
2. Incident Analysis ——— *PERFORM AS APPROPRIATE*.
3. Requests From EGI CSIRT ——— *FOLLOW UP* ***WITHIN FOUR HOURS***.

6 — Debriefing

1. Post-Mortem Incident Report ——— *PREPARE AND DISTRIBUTE via "site-security-contacts@mailman.egi.eu"* ***WITHIN ONE MONTH***.

7 — Normal Operation Restoration

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