Process för hantering av incidenter som påverkar IdP(er) i SWAMID:

1. Organisationen som påverkats informerar SUNET CERT och SWAMID Operations (operations@swamid.se) om vad som hänt omedelbart efter att incidenten upptäcks.
1a. SWAMID operations informerar noc@sunet om den inträffade incidenten.
1b. SWAMID operations stänger av IdP(er) från SWAMID WebSSO och/eller eduroam i förekommande fall. SWAMID Operations fattar beslut om hur incidenten ska hanteras i detta avseende.

2. SUNET CERT gör analys av incidenten och informerar SWAMID Operations löpande.

3a. SWAMID Operations informerar med hänsyn tagen till pågående utredning alla påverkade parter i SWAMID samt operationella kontakter för eventuella interfederationer.
3b. SWAMID Operations informerar fortlöpande noc@sunet.

4. Om intrånget är av allvarlig art så kan medlemskap revokeras enligt SWAMID policy.

5. Organisationen återställer operationell säkerhet och informerar SUNET CERT och SWAMID Operations löpande om arbetet.

6. SUNET CERT genomför en audit av operationell säkerhet och informerar SWAMID Operations när audit är godkänd.

7. Organisationen säkerställer att den av SWAMID godkända identitetshanteringsprocessen är uppfylld för alla användare som exponeras mot SWAMIDs tekniska profiler (WebSSO och eduroam).

8a. Om medlemskap blev revokerat i (3) så måste organisationen söka nytt medlemskap
8b. Tillfälligt avstängda IdPer från punkt (1b) läggs åter in i SWAMID WebSSO och/eller eduroam, baserat på giltigt medlemskap samt återställd identitetsprocess (7) samt efter godkänd SUNET CERT audit.

9. SWAMID Operations informerar berörda parter (se punkt 3) om att ärendet är hanterat.

Process för hantering av incidenter som påverkar SP i SWAMID:

1. Organisationen som påverkats informerar SWAMID Operations om vad som hänt omedelbart efter att incidenten upptäcks.
2. SWAMID operations stänger av SP från SWAMID WebSSO och/eller eduroam i förekommande fall.
3. SWAMID Operations informerar alla påverkade parter i SWAMID samt operationella kontakter för eventuella interfederationer.
4. Organisationen återställer operationell säkerhet och informerar SWAMID Operations.
5. SP läggs in i SWAMID WebSSO och/eller eduroam.
6. SWAMID Operations informerar berörda parter (se punkt 2) om att ärendet är hanterat.