Privacy and Security Breach

DSOP Control Information Common Standard - Operational processes
V 2.0

Change Log

| Version	Change description	Approved by
2.0	Approved version	Referansegruppe Bank

Introduction

DSOP

- This document aims to give clear instructions to anyone who discovers a privacy or security breach.

- If there is any uncertainty of the definition of your error, the criticality of your breach or you need help with understanding this document, please reach out to dsop@bits.no

Glossary

Term	Norwegian	English
Action Group	En gruppe mennesker som midlertidig er samlet, enten på samme sted eller digitalt, for å løse hendelsen.	A group of people gathered temporarily, in person or digitally, to solve the incident.
Affected party	Parten eller partene som er påvirket av bruddet.	The party/parties that the breach impacts.
Reporter	Parten som rapporterer bruddet.	The party that reports the breach.
Breach	Personvern- eller sikkerhetsbrudd.	Privacy or security breach.
Incident	En hendelse. Brukes i tilfeller hvor en part ikke nødvendigvis ønsker å dele detaljert informasjon med andre DSOP-aktører.	The term is used when a party doesn't necessarily wish to share detailed information about the breach with other DSOP-participants.

DSOP Control Common Standard – Privacy and security breach
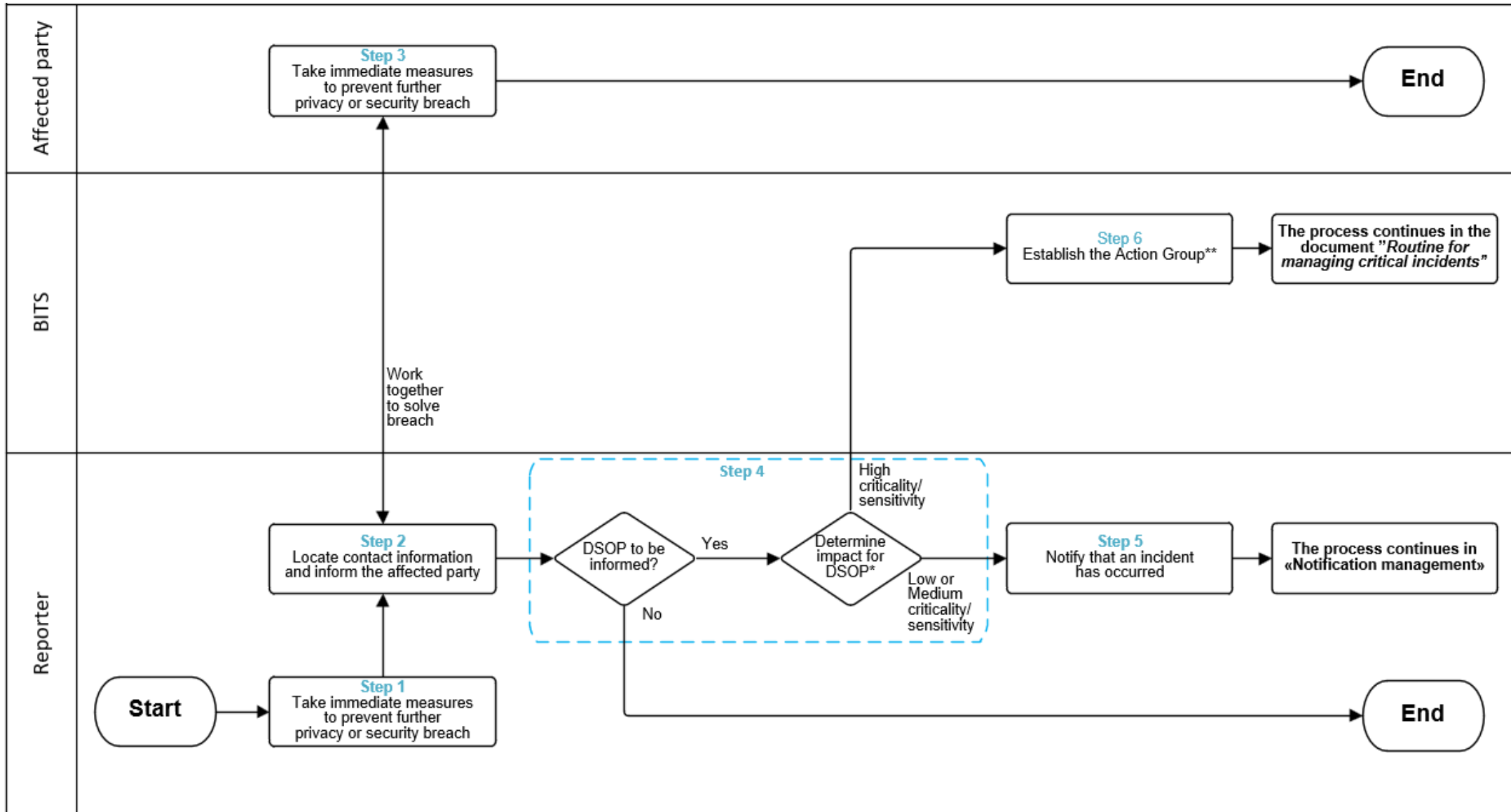
* In accordance with appendix 3 of the agreement - "SLA og varslingsrutiner" – Chapter 2.2.1 and 2.4
** In accordance with appendix 3 of the agreement - "SLA og varslingsrutiner" – Chapter 2.4.3

5

Step 1

Take immediate measures to prevent further privacy or security breach

- The Error Reporter evaluate the impact of the privacy or security breach

- If necessary, the service will be closed for the affected party until the privacy or security breach is resolved.

Step 2

Locate contact information and inform the affected party

- The contact information is available in the agreement*
  - The affected party is expected to work together with the Reporter to solve the incident.

- Once either party determines the incident's impact level, the reporter decide when to proceed to Step 4.

* Appendix 3 of the Agreement - "SLA og varslingsrutiner" - Chapter 2.4.2

Step 3

Take immediate measures to prevent further privacy or security breach

■ If necessary, the access to the service will be closed until the security or privacy breach is resolved.
– The affected party is expected to work together with the Reporter to solve the incident.

■ Once either party determines the incident's impact level, the reporter decide when to proceed to Step 4.

Step 4

- Step 4 contains two decisions.

1. Decide whether other DSOP-participants should be made aware of the breach.
   - If no, the process ends.
   - If yes, move to the next decision.

2. Determine what level of impact the incident have on the DSOP community*.
   - If low/medium, move to Step 5.
     - Bits will share relevant information with the other DSOP-participants.

   - If high, move to step 6.
     - Bits establishes *Action Group*

* In accordance with appendix 3 of the agreement - "SLA og varslingsrutiner" – Chapter 2.2.1 and 2.4

Step 5

Notify that an incident has occurred

■ The Reporter decides what granularity of information to be shared with the other DSOP-participants.

■ The reporter will use the "*Notification management*" routine.
  − The content of the notification may include:
    • That a DSOP-participant has been affected.
    • The extent of the security or privacy breach/incident.
    • What measures the recipient should take in the immediate or longer term.

Step 6

Bits establishes *Action group*

■ Bits will establish the *Action Group* in accordance with the agreement*.

■ The documentation for how the *Action Group* is formed, and how it resolves a breach is described in the document "*Routine for managing critical incidents*", that is distributed with appendix 3*.
  – A copy can be obtained by contacting Bits at support.dsop.no.

* Appendix 3 of the agreement - "SLA og varslingsrutiner" - Chapter 2.4.3