Information Security Incident

Upstream Outcomes Policy

(Supporting Bridgit Care & Upstream health Business Units)

Author: D Crombie
Date: 04/04/2022
Version: 2.0

Information and technology
for better health and care

Contents

1 Background

This policy is based on NHS Digitals example policy and aligns to the recommendations and approach adopted by NHS Digital. This is based on the NHS Digital template dated 23rd May 2017.

2 Approval / update history

Version ID	Description	SIRO Approval
1.0	Initial version for release	08/10/2018 : Darren Crombie
2.0	Updated version following 2022 review	05/04/2022 : Darren Crombie

Terminology

Term	Definition
SHALL	*This term is used to state a **Mandatory** requirement of this policy*
SHOULD	*This term is used to state a **Recommended** requirement of this policy*
MAY	*This term is used to state an **Optional** requirement*

Policy

*The Information Security Incident Policy **shall** be used to produce, implement, test and manage the information security incident procedure for <insert name of organization> incidents (including IT incidents and suspected data loss/breaches (electronic and physical).*

Information Security Incidents

- *An Information Security Incident is an event, or chain of events, that could compromise the confidentiality, integrity or availability of information. Examples of information security incidents can include but are not limited to:*
  - *Potential and suspected disclosure of NHS or other UK Government information to unauthorised individuals.*
  - *Loss or theft (attempted or actual) of paper records, data or IT equipment on which data is stored.*
  - *Disruption to systems and business processes.*
  - *Inappropriate access controls allowing unauthorised use of information.*
  - *Attempts to gain unauthorised access to computer systems, e.g. hacking.*
  - *Records altered or deleted without authorisation by the data 'owner'.*
  - *Virus or other malicious (suspected or actual) security attack on IT equipment systems or networks.*
  - *'Blagging' offence where information is obtained by deception.*
  - *Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing NHS sensitive or other UK Government information left unlocked in accessible area.*
  - *Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information.*
  - *Human error such as emailing data by mistake.*
  - *Covert or unauthorised recording of meetings and presentations.*
  - *Damage or loss of information and information processing equipment due to theft, fires, floods, failure of equipment or power surges.*
  - *Deliberate leaking of information.*

- *Insider fraud.*

Information/Data Breach

- *An information/data breach is a security incident where sensitive, protected or confidential data has intentionally or unintentionally been released or obtained by persons who are not authorised to view or access it.*

Information Security Incident Management

- *Upstream Outcomes **shall** be able to manage incidents affecting NHS or other UK Government information assets from identification and analysis, through to response, resolution and recovery.*
- *The Upstream Outcomes information security incident management process **shall** be fully documented to be able to handle different types of information security incident.*

Information Security Incident Reporting

- *<Insert name of organization> **shall** ensure that any incident that could potentially affect the security of information is identified and managed appropriately.*
- *The incident **shall** be reported to the National Service Desk via telephone*
- *The process **shall** be simple, clear and easy to follow. It **should** follow the below guidelines:*
  - *Use a single point of contact for telephone reporting of incidents with internal and external telephone number (National Service Desk)*
  - *Use a simple reporting form for incident reporting. The reporting form **should** be easily available via the Upstream Outcomes intranet/IT system and capture the required information, which is suggested to be no more than:*
    - *Date*
    - *Location*
    - *Short summary of what occurred*
    - *Type of incident – e.g. e-mail, lost USB device or paper*
    - *Contact details for obtaining further information*
  - *Everyone within Upstream Outcomes is responsible for reporting security incidents. All personnel **shall** be made aware of what constitutes an incident and how to report them via the Education and Awareness process.*
  - *Information security incident management **shall** be incorporated into all third party and outsourced contracts.*

Within Upstream we produce a simple one page form.

Information Security Incident Analysis and Response

- *Upstream Outcomes **shall** ensure that all incidents are assessed as soon as possible, so that the most appropriate course of action and a priority can be given for their resolution. The response to an incident is likely to require the skill and expertise of various groups within <insert name of organization> (IT, operations, legal and human resources) as well as external agencies (police authority, forensic specialists).*

- *The analysis, by the specialists handling the incident, **shall** include the following processes:*
  - *Assessment of the severity of the incident against Upstream Outcomes : severity scaling.*
  - *Identification of type of incident – paper loss, e-mail, portable IT media.*
  - *Assessment of scale of incident in terms of data size – e.g. Gb of data or number of pages lost or distribution list.*
  - *Identification of classification or type of data – e.g. OFFICIAL, OFFICIAL-SENSITIVE, NHS Confidential or NHS Protect.*
- *All actions and decisions made during the response to incidents **shall** be recorded.*

Collection of Evidence

- *Upstream Outcomes **shall** ensure that if an incident is suspected to be caused as a result of a criminal or if legal action is anticipated, then further advice must be obtained from the National Service Desk and steps taken to ensure that any evidence necessary for a successful prosecution is not intentionally or accidentally destroyed in accordance.*

Learning from Incidents

- *Upstream Outcomes **shall** ensure that all incidents are monitored to establish whether there are any trends that could be addressed. For all major incidents, a post incident investigation of the information security incident and the actions taken to resolve the incident **shall** be conducted to:*
  - *Determine the root cause of the incident.*
  - *Quantify its impact on Upstream Outcomes.*
  - *Minimise the possibility of recurrence.*
  - *Improve future responses.*

Follow on Actions

- *Upstream Outcomes **shall** ensure that the necessary remedial action is taken to ensure that information security incidents do not recur. This **shall** involve the review of existing security controls, IT training and awareness, contractual and service level agreements.*

Specific Reporting Requirements

- *The following information security incidents **shall** be assessed and where appropriate reported as follows:*

Incident Type	***Reported To***
Technical events (hacking, Denial of Service, malware, hardware or software vulnerabilities	*GovCertUK for information sharing purposes or national security investigation*
Criminal event	*Police authority*

Loss of personal data	*Information Commissioner's Office, Dept of Health and respective Caldicott Guardian*
Compromise of CESG/NCSC (National Cyber Security Scheme) approved Crypto products or Keymat	*CINRAS (Comsec Incident Notification Reporting and Alerting Scheme)*

3 Key Words

Analysis, Data Breach, Information Security Incident, Reporting