

Security Incident Procedure

Adopted by the Management Committee on 2 July 2018

Last Updated June 2019 – See Management Committee Minutes for details of changes

Introduction

The New Dawn Child Contact Centre will manage any security incidents. This procedure details the actions and roles required when a security incident occurs. It is provided as guidance to staff.

All security incidents are recorded. Security incidents are issues that potentially impact on the confidentiality, integrity or availability of the centres systems or services.

Procedure

Security incidents will be reported to the Chair of the Management Committee or Co-Ordinator (or their delegate).

On receipt of the security incident report, the Chair of the Management Committee or Co-Ordinator will take the following actions:

1. Receive notification that an incident has occurred from a member of staff, volunteer or service user e.g. stolen laptop, or complaint
2. Confirm the type of incident and gather any additional information required by the ICO
3. Log the incident including a brief description, time and date of the incident, who notified the incident and assign a priority High, Medium or Low
4. Investigate the incident
5. Diagnose the incident and identify any actions required to resolve the incident see Incident Types and Responses. Where necessary escalate to ICO as soon as possible and within 72hrs. Notify any affected individuals.
6. Incident Resolved - update incident record with details of actions taken and results of an investigation regarding the cause whether this was human error or a systemic issue
7. Record any details of how recurrence can be prevented – whether this is through better processes, further training or other corrective steps.
8. Close incident



Responses

The standard responses are:

Personal Data Leakage Response

If the incident results in the loss of personal data as defined in the DPS (2018) / GDPR then it must be reported to the ICO.

Examples of a data breach personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

Under the GDPR there is a requirement for organisations to report a personal data breach that affects people's rights and freedoms, without undue delay and, where feasible, not later than 72 hours after having become aware of it. Organisations should be aware that the ICO will have the ability to issue fines for failing to notify and failing to notify in time. Fines can be avoided if organisations are open and honest and report without undue delay, which works alongside the basic transparency principles of the GDPR.

Serious breaches should be reported to the ICO using our DPA security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give you advice about what to do next.

Further information can be found at:

https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

Criminal Attack Response

If the incident is a potential attack incident, the incident will be reviewed and if an attack is confirmed it should be reported as such to the customer who will report it to the relevant law enforcement body. The New Dawn Child Contact Centre will zip and sign the relevant evidence, collected from logs etc. earlier. This evidence will be made available to the customer as required, subject to confidentiality undertakings (it will contain non-customer specific sensitive information). The complete pack will be preserved for subsequent law enforcement action.

Denial of Service (DoS) Response

This has become an increasing threat recently, often manifested as a distributed denial of service (DDoS) attack, which is more difficult to combat. Access to bot-nets is becoming increasingly widespread so that individuals with grievances have access to facilities hitherto only available to criminal organisations. The attack could be directed at New Dawn Child Contact Centre or New Dawn Child Contact Centre could be subject to collateral damage due to attacks on adjacent services. DoS and particularly DDoS attacks can result in:

- The New Dawn Child Contact Centre website being unable to respond to legitimate transactions as they are swamped by a flood attack. This would be a direct attack from a low capacity resource
- The hosting site being forced to suspend the service to enable other services on their site to continue. If this is a direct attack, New Dawn Child Contact Centre would be suspended, if New Dawn Child Contact Centre was suffering collateral damage this would re-open New Dawn Child Contact Centre
- The ISP switching off access to the New Dawn Child Contact Centre in order to prevent their service from being overwhelmed. Again, if this is a direct attack, New Dawn Child Contact Centre would be suspended, if New Dawn Child Contact Centre was suffering collateral damage this would re-open New Dawn Child Contact Centre

For a DoS attack or low capacity² DDoS, action from the hosting provider to block traffic from specific incoming IP addresses should be taken. Arrangements for this action will be made with each hosting site.

² Where the number of attacking IP addresses are such that all the attacking addresses could be filtered.

For DDoS, the customer should be contacted and, subject to their agreement Emergency DDoS protection should be put in place. As this is chargeable, the customer's agreement and order must be obtained before invoking the service.

The New Dawn Child Contact Centre will maintain a list of suitable service providers, contact details and costs.

Malware Discovery

Where malware is discovered by routine application of anti-malware measures, this should be logged.

Web Exploit

In most cases, this will be a new exploit. We need to cover, routinely, the OWASP exploits (see <http://www.ibm.com/developerworks/library/se-owasptop10/index.html>), although some variants may need modified responses. On discovery of a web exploit we will devise and put into place an emergency fix / procedure to block the exploit. We will check against the OWASP list if the exploit is known. If it is not, we will inform OWASP of the exploit, providing details as required. If it is a deliberate act, we will invoke our Criminal Attack Response, including the session logs in our evidence pack.

Definitions

Incidents will be classified according to their impact on the New Dawn Child Contact Centre systems or services.

Level	Impact
High	Actual breach effecting the availability, integrity or confidentiality of the New Dawn Child Contact Centre critical information assets.
Medium	Vulnerability discovered which, if exploited could give rise to a data breach
Low	Other types of security incident

ICO data required

A description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

End of Security Incident Procedure