Responding to Information Security Incident Reports Procedure

Version number: 1.0

Publish date: 16-05-2018

Document control	
Prepared by	Mike Moore, Managing Director
Authorised by	Upper Management
Physical Copy location(s)	Operations Folder
Source Copy Location(s)	Dropbox - GDPR123\Documents\Final Documents
Published Copy Location(s)	www.Dephoto.biz\GDPR
Other Referenced Documents	Communication Procedure
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Responding to Information Security Incident Reports Procedure			
Description	To ensure that all actual or potential information security incidents are responded to efficiently, enabling the company to react quickly and effectively to minimise the impact.			
Created by	Mike Moore			
Date Created	16-05-2018			
Maintained by	Upper Management			
Version Number	Modified By	Modifications Made	Date Modified	Status
1.0	Mike Moore	First creation	16-05-2018	Published

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Contents

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Purpose

DE Photo (Franchising) Ltd (referred to as the company here after) uses many methods to detect possible security incidents. The purpose of this procedure is to ensure that all actual or potential information security incidents are responded to efficiently, enabling the company to react quickly and effectively to minimise the impact.

The aims of the procedure are as follows:

- To quickly enact procedures and plans
- Determine whether further controls or actions are required
- Evaluate the information security management system and make necessary improvements

All information security incidents will be dealt with by the information security dept. who will review and advise on incidents and make recommendations on appropriate follow up and corrective action. Specialised input will be sought where necessary using authorised contracted third parties.

Prerequisites

For this procedure to be followed the following conditions need to be met:

- All parties need to be aware of their roles and responsibilities.
- All parties have had the relevant training and the training is current and up to date.
- The following policies and procedures are current and available:
    - DE-GDPR-0055 - Communications Procedure

Conditions

- A security weakness or event report has been submitted to the information security dept.
- A complaint has been escalated to the security response phase

Outcomes

- Reported security weaknesses and events are acknowledged
- Reported security weaknesses and events are verified
- Reported security weaknesses are responded to with appropriate measures

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Processes

Acknowledging reports sub-process

1. The IT Security department should acknowledge the receipt of a security weakness or event report. The format of the report should be as shown below in table 1.1, if any fields are missing the party submitting the report should be informed and requested to resubmit the form with all the information.

Date:	{The date the event occurred/weakness was discovered}
Time:	{The time the event occurred/weakness was discovered}
Affected Places:	{the physical locations of equipment that were affected by the event/weakness}
Name of responder:	{The designated Party for responding to the report}
Position:	
Classification:	{A value from 1 to 5 indicating the impact of the event/weakness}
Contact Details:	{A contact email/number/other contact details of the person reporting the weakness/event}
Source of information:	{Where the information about the event/weakness came from}
Description:	{Details about the event/weakness}
CVE ID(s):	{Known CVE IDs connected to the weakness/event}
Verification status:	{Whether the information in this report has been verified}
Corrective actions:	{Actions that will need to be taken to respond to the reported weakness/event}
Date reviewed:	{Date to review this report and corrective actions}
Date completed:	{The date that the corrective actions have been verified as complete}

Table 1.1: Example security weaknesses or event report

2. The report should be moved from the Submitted folder:
   Dropbox: \GDPR123\Documents\File Locations\Submitted
   to the Action folder:
   Dropbox: \GDPR123\Documents\File Locations\Action

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824

Verifying the report sub-process

1. The responder should begin with information sources listed in the report making sure that these sources match the weakness or event that has been reported and that it is not a false positive.
2. Where only one information source was given the responder should verify the report with another source.
3. All submitted reports should have an impact classification based on table 2.1. The responder should perform their own analysis and make sure that the correct impact classification has been applied.

Level	0	1	2	3	4	5
	Low	**Medium**		**High**		
	No significant damage to reputation, organization or data	Damage to employee supplier reputation	Damage to departmental reputation	Damage to service availability or service reputation	Damage to product reputation	Damage to organization reputation
	External interest unlikely	Possible external interest	Definite external interest	Low key local public interest	National or local interest	National Interest
	Not a data breach	Potential breach of data	Risk assessed as high	Serious breach of data	Serious breach of data including personal information	Serious breach of sensitive personal information
	Effects a non-production system	Less than 5 records potentially affected and low risk due to security measures	Up to 50 records potentially affected and high risk due to inadequate security measures on data records	Up to 100 records potentially affected	Up to 1000 records potentially affected	Over 1000 records potentially affected

Table 2.1: Impact classification table

Determining appropriate response sub-process

1. Once the report has been verified, the response party should draw up appropriate response measures. To start with, the responder should map a process for the weakness or event.
2. The next step is to evaluate any existing security measures to identify where they have failed, how the weakness/event occurred and what improvements could have prevented the issue.
3. Using the process, consider all security measures that would end the process before it impacts information security.
4. Evaluate the changes to existing measures and possible new security measures for feasibility, practicality, cost and their impact on other systems.
5. Make change requests for measures that meet the requirements. Where the impact classification is 3 or higher, an emergency change control board request should be made instead.

Implementing the appropriate response sub-process

1. Once the appropriate response has been decided and approved, a schedule of implementation should be created.
2. Scope, schedule and details of the change must be communicated as stated in the Communication Procedure to all relevant and affected parties.
3. Before implementing the change, the affected systems should be backed up and where necessary all documentation should be verified.
4. Next, the response should be enacted according to the schedule.

Reviewing the effectiveness of the response sub-process

1. Once the appropriate response has been implemented, all affected systems to undergo security testing to make sure that weaknesses have been fixed and the response has not inadvertently created new vulnerabilities.
2. Monitoring should be set up as stated in the Monitoring Procedure.
3. After a fixed amount of time, the results of the monitoring and records of any further incidents should be reviewed

Documenting the response sub-process

1. All sub-processes should be documented
   a) The acknowledgement sub-process should have copies of the acknowledgement emails stored in:
   Dropbox: \GDPR123\Documents\File Locations\Acknowledgement
   b) The verification sub-process should have a record of the verification status in the security weaknesses and events log stored in:
   Dropbox: \GDPR123\Documents\File Locations\Action
   c) The determining response sub-process should have change requests located in
   Dropbox: \GDPR123\Documents\File Locations\Change Control
   and risk assessments in:
   Dropbox: \GDPR123\Documents\File Locations\Risk Assessments
   d) The review process should include scan results stored in an appropriate secure location and log results stored in the relevant systems.

Management and Review

This policy should be reviewed as scheduled once annually unless performance indicators, changes to legislation or the organisation necessitate it.

Last Review Date: 16/05/2018

Next Review Date: 16/05/2019

Unit 19 Lambs Business Park, South Godstone, RH9 8LJ | www.DEphoto.biz | 01342 894519
DE Photo (Franchising) Ltd. | Company Reg No. 5160591 | ICO Reg No. Z2569824