Reporting Information Security Weakness and Events 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	Monitoring Policy
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Reporting Information Security Weakness and events procedure			
Description	To ensure that all actual or potential information security incidents are reported 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 reported 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. Specialist 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.
- Monitoring and measurement systems are in place to detect and notify of suspected incidents as defined in the Monitoring Policy.
- The reporting parties needs access to:
  Dropbox: \GDPR123\Documents\Final Documents

Conditions

This procedure should be followed if there are signs of a breach or incident. Examples include but are not limited to:

- A malware or suspected malware infection on any devices.
- If a supplier suffers a breach.
- If any of the monitoring systems detect unauthorized access.
- If any parties have knowledge of undisclosed information.
- If there is a physical or suspected physical break in to the premises.
- If equipment is lost or stolen.
- If policies and procedures aren't complied with.

Outcomes

- Suspected incidents are identified
- Incidents reported in an effective and efficient manner to the correct teams.
- Records of the reports are documented
- Further actions are determined where necessary

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

Identifying a weakness or event sub-process

1. New information has become available to a party within the company from a source; examples of sources include but are not limited to:
   a. Information submitted by contracted third parties
   b. Information submitted from a complaint
   c. Information from one of the monitoring systems defined in the Monitoring Policy.
   d. Information published by the press
   e. Information from tests or scans
   f. Information from reviews

2. This information must concern information security or data protection; examples of such information include but are not limited to:
   a. Information processed or controlled by the company that is incorrect, inaccurate or incomplete.
   b. One or more of the company's systems for interacting with controlled or processed data was unavailable.
   c. Information relating to a suspected breach.
   d. Information that the rights of a data subject are not being protected
   e. Information that information required to be provided to data subjects under Regulation (EU) 2016/679 (GDPR) is not being supplied in full.
   f. Objections to lawfulness or fairness of processing.
   g. Objections to consent gathering procedures.
   h. Concerns about the obligation to protect children.
   i. Concerns about the measures to protect data
   j. Concerns about the physical security of the company premises
   k. Stolen or missing equipment
   l. Non-compliance with company policies and procedures

3. This information should classified using the classifying a weakness or event sub-process and reported using the reporting a weakness or event sub-process.

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

Classifying a weakness or event sub-process

1. The information that identifies an information security weakness or event should be classified according to table 1.1 (below)

Level	0	1	2	3	4	5
	Low	**Medium**		**High**		
	No significant damage to reputation, organisation or data	Damage to employee supplier reputation	Damage to departmental reputation	Damage to service availability or service reputation	Damage to product reputation	Damage to organisation 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 1.1: Information security classification table

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

Reporting a weakness or event sub-process

2. Open a copy of the Security Weakness and Events Template form (table 2.1) found in the location: Dropbox: \GDPR123\Documents\Final Documents

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 the corrective actions}
Date completed:	{The date that the corrective actions have been verified as complete}

Table 2.1: Incident Report Template

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

3. Save this report to the location:
   Dropbox: \GDPR123\Documents\File Locations\Saved Reports
   with the file name {date}-{classification level}-{weakness or event}-{initials}-{number of reports for that day}. For example, if John Smith wishes to submit a report for a level 3 weakness on November 15th and has made no other reports that day then the file name will be: 15NOV17-3-Weaknesses-JS-0001.

4. A copy of this report should be sent via email to IT Security department, Michael Newnham

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