Security Response Plan Policy

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	Information Security Policy
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners

Version Control				
Title	Security Response Plan Policy			
Description	Outlines the approach to responding to an information security event. This policy requires management to financially support and diligently attend to security response planning efforts in order to ensure that resulting plans can succeed.			
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

This policy is a supporting policy of the Information Security Policy so the purpose of this policy is the same, to secure information. DE Photo (Franchising) Ltd (referred to as the company here after) take information security very seriously. This policy outlines the approach to responding to an information security event. This policy requires management to financially support and diligently attend to security response planning efforts in order to ensure that resulting plans can succeed.

This policy defines the requirements for a baseline security response plan to be developed and implemented by the company that will describe the process to respond to a security incident.

Scope

This policy is directed to the Management Staff who are accountable to ensure that the plan is developed, tested and kept up-to-date and key stake holders who have a vested need for information security.

Definitions

- Disaster – An event that causes disruption to the company's critical systems
- Baseline – An indication of the normal state of a system
- Critical Service – A service that would cause serious impact (for example, financial, contractual, reputational, etc.) to the company.

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

Policy

Contingency Plans

When creating security response plans, the following will be given due consideration and incorporated where necessary:

- Emergency Response Phase - Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Delegation of Authority: Describe the flow of responsibility when normal staff are unavailable to perform their duties.
- Data Inventories: Where is sensitive data and propriety information located and what are the obligations on confidentiality, integrity and availability?
- Mitigating actions: What actions can be taken to mitigate the risks of the affected data?
- Response Timelines: What needs to be accomplished when.
- Breach Notification: Who needs to be notified? What are the company's notification obligations?
- Collection of evidence: What steps are taken to preserve and collect evidence of the security incident?
- Communication Management: Who is in charge of giving information to various parties and is there a need for a press release?

After creating the plans, it is important to test them by running through the response process.

Management should set aside time to test implementation of the Security Response Plan.

Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

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

Compliance

Monitoring and Measurement

The information security dept. will verify compliance to this policy through various methods, including but not limited to, reviewing meeting minutes, testing response plans and interviewing staff.

Compliance

Compliance with this policy is not optional. Any employees or franchisees that are found to have violated this policy will be subject to the disciplinary terms detailed in the Data Protection Policy in line with the severity of the offence and the damages caused.

Contractors or related third parties that are found to have violated this policy will be liable for damages as laid out in the contract terms and may be subject to legal actions.

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