Encryption 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, Physical Security Policy, Data Protection Policy
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Encryption Policy			
Description	The company's approach to and use of encryption is defined alongside the encryption methods that should be used.			
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

Contents

Purpose 3

Scope 3

Definitions.. 3

Policy 4

Encryption Standards 4

Encryption on data at rest.. 4

Encryption on data in transit 4

Encryption Keys and Recovery 4

Compliance 5

Compliance Measurement.. 5

Exceptions.. 5

Non-Compliance 5

Management and Review 5

Purpose

This policy is a supporting policy of DE Photo (Franchising) Ltd (referred to as the company here after) Information Security Policy and so has the same purpose of securing information. In this policy, the company's approach to and use of encryption is defined alongside the encryption methods that should be used. Encryption is used as method to reduce the risks associated with a data breach as recommended as an appropriate technical measure in Article 32 Paragraph 1 of Regulation (EU) 2016/679 (GDPR).

Scope

This Policy applies to employees, franchisees, contractors, consultants and other workers using equipment or accounts on behalf of the company. This guideline applies to encryption of all devices including but not limited to laptops, desktops, tablets, mobile phones and storage devices. This policy also covers data in transit.

Definitions

Encryption keys – A random string used to encrypt and unencrypt data.

Hashing – the processing of using a mathematical algorithm to hide data in a string of fixed size.

Salt – The fixed size string used in hashing.

Policy

Encryption Standards

The company should use encryption software and services that support a minimum of AES256. This meets the recommendations of the National Cyber Security Centre (NCSC) and other security organisations and has no known exploitable vulnerabilities.

Encryption on data at rest

All desktops, laptops and devices where possible should have full disk encryption.

Encryption on data in transit

All digital data being moved must be encrypted.

Where data is being transmitted over the Internet, the service must be secured by HTTPS to connect with a suitable certificate.

Where possible, emails should be sent encrypted using a secure digital signature.

Any other methods of moving data should be brought before the information security team so that they can make a decision on the encryption methods.

Encryption Keys and Recovery

When using encryption, there is a danger that data may be lost if encryption keys are not known to handle decryption. All encryption keys, recovery keys, IDs, signing requests and cryptographic components must be documented and stored both physically in a secure fire proof safe (refer to the Physical Security Policy on how to store sensitive physical documents) and electronically within a secure encrypted store and not within their own encrypted volumes.

Compliance

Compliance Measurement

Compliance to this policy is determined through various methods, including but not limited to, periodic training, internal and external audits, and feedback to the information security dept.

Exceptions

Any exception to the policy must be approved in advance by the information security dept and noted in this policy.

Non-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