Information Security 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	Communication Policy, Acceptable Use Policy, Boundary Device Protection Policy, Clean Desk Policy, Disaster Recovery Policy, Email Policy, Password Policy, Removable Media Policy, Security Response Plan Policy, Encryption Policy
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Information Security Policy			
Description	To ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.			
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

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

Scope

The documents in the Information Security Policy apply to all information assets which are owned by DE Photo (Franchising) Ltd (referred to as the company here after), used by the company for business purposes or which are connected to any networks managed by the company.

The documents in the Information Security Policy apply to all information which the company processes, irrespective of ownership or form.

The documents in the Information Security Policy apply to all employees of the company and any third party contractors who may process information on behalf of the company.

Structure

The Information Security Policy document set is structured in accordance with the control guidelines set out in the industry standard ISO 27001.

This top level document lists a set of sub-policy documents which together constitute the Information Security Policy of the company. All of these documents are of equal standing. If any inconsistency is found between this policy and any of the sub-policies, this policy will take precedence.

Each of the sub-policy documents contain high-level descriptions of requirements and principles. They do not, and are not intended to include detailed descriptions of policy implementation.

Such details will, where necessary, be supplied in the form of separate procedural documents and referenced from the relevant, individual sub-policy documents.

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

Supporting Policies

Name	Filename
Acceptable Use Policy	DE-GDPR-0016
Boundary Device Protection Policy	DE-GDPR-0018
Clean Desk Policy	DE-GDPR-0019
Email Policy	DE-GDPR-0020
Password Policy	DE-GDPR-0022
Removable Media Policy	DE-GDPR-0023
Security Response Plan Policy	DE-GDPR-0024
Encryption Policy	DE-GDPR-0021

Governance and Principles

1. Information will be protected in line with all relevant company policies and legislation, notably those relating to data protection (DPA, GDPR, ISO 27001), human rights and freedom of information.
2. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
3. Information will be protected against unauthorised access.
4. Compliance with the Information Security Policy will be enforced.
5. All information in the policy is set to comply with regulations and legislation set out by ICO Standards and Definitions.

All devices mobile or fixed must be updated and maintained according to a regular schedule.
For specific details regarding standards within the IT Security Policy, please refer to the sub-policies referred to within this document.

Definitions

“Up to date” is used when software or firmware patching is referred to.
“Antivirus” refers to recommended software used to mitigate the risk of virus and malware infections and provides real time protection.

For further information and specific details regarding definitions, please refer to the sub-policies referred to within this document.

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

Roles and Responsibilities

Senior Management:

- Responsible for the suitability, adequacy and effectiveness of the information security policies, procedures and enforcement.
- Establish the Information Security Policy, procedures, objectives and plans
- Communicate the importance of meeting the information security objectives and the need for continual improvement
- Determine and provide resources to plan, implement, monitor, review and improve information security and management e.g. recruit appropriate staff, manage staff turnover
- Manage risks to the organisation
- Conduct reviews of information security at planned intervals, to ensure continuing suitability, adequacy and effectiveness
- Establish a continual improvement policy with respect to information security for the organisation
- Ensure that arrangements that involve external organisations having access to information systems and services are based on a formal agreement that defines all necessary security requirements.

Data Protection Officer:

- Responsible for ensuring policies conform to the requirements of current legislation including DPA and GDPR; and for reporting on the performance of policy to management.
- Communicate the Information Security Policy to all relevant personnel and customers where appropriate
- Implement the requirements of the Information Security Policy
- Manage risks associated with access to the service or systems
- Ensure that security controls are documented
- Quantify and monitor the types, volumes and impacts of security incidents and malfunctions
- Establish and maintain a continual improvement action list and report on improvement activities
- Ensure that procedures are in place to define the recording, prioritization, business impact, classification, updating, escalation, resolution and formal closure of all security incidents
- Ensure that all staff involved in incident management shall have access to relevant information such as known errors, problem resolutions and the configuration management database
- Manage and classify major incidents according to a process
- Arrange service review meetings on a regular basis.

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

Information Asset Owners:

- Responsible for specific, named information assets
- Maintain and review security controls for allocated asset(s)
- Participate in risk assessments concerning their asset(s)
- Ensure the relevant entry in the asset inventory is kept up to date
- All employees of the organisation are trained in their information security responsibilities and are held accountable.

Auditor(s): Responsible for assessing and evaluating the effective usage and enforcement of policy.

Managing Agent: Responsible for physical security, e.g. buildings etc.

Human Resources: Overall responsibility for the staff.

Information Security Policy Detail

Acceptable Use Policy

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the company's established culture. The company is obligated to protect employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the company.

These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Effective security is a team effort involving the participation and support of every the company employee and affiliate who deals with information and/or information systems.

It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. For detailed information, please consult the separate Acceptable Use Policy.

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

Antivirus/Anti-Malware Device Protection Policy

A virus and or malware is a piece of code, script or application with malicious intentions, usually designed to destroy or corrupt information, steal user data or adversely impact the usage of IT systems.

Potential sources of viruses include shared media such as USB memory sticks, electronic mail (including, but not limited to, files attached to messages), malicious code embedded in websites and software or documents copied over networks such as the internal network or the Internet.

An infection by malicious software is almost always costly to the organisation whether through the loss of data, time to recover data and the delay of important work. In addition, any malicious software or code spread from the organisation could potentially lead to serious issues of damage to reputation, client confidentiality and/or fines/investigation from a governing body.

- All computers connected to the organisation's network must run an approved, licensed and up-to-date anti-virus product that continually monitors for malicious software.
- Currently all computers must run managed virus protection software.
- Privately owned computers that connect to the organisation's network must be equipped with an appropriate anti-virus product.
- The company reserves the right to disconnect any machine from the network if an infection is found or suspected.
- Any device used to access data owned by or relating to the company's business, staff or clients must have up to date and appropriate anti-virus and anti-malware software installed and operational.

All staff and third party contractors are responsible for taking suitable measures to protect against virus infection.

For further information, please see the Antivirus Policy for in-depth policy information and procedures.

Boundary Device Protection Policy

Firewalls are an essential component of the company security infrastructure. Firewalls are defined as security systems that restrict network connectivity and network services. Firewalls establish a control point where access controls may be enforced. Connectivity defines which computer systems are permitted to exchange information.

For further information, please see the Boundary Devices Protection Policy for in-depth policy information and procedures.

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

Clean Desk Policy

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or when an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee awareness about protecting sensitive information.

For more information, please refer to the separate Clean Desk Policy.

Email Policy

Electronic mail (email) is pervasively used in almost all industries and is often the primary communication and awareness method within an organisation. At the same time, misuse of email can pose many legal, privacy and security risks; thus it's important for users to understand the appropriate use of electronic communications.

For detailed information regarding the use of email, please refer to our Communication Policy.

Encryption Policy

Encryption Management, if not done properly, can lead to secure sensitive data being compromised. While users may understand it's important to encrypt certain documents and communications, they may not be familiar with minimum standards for encryption. For further information, please refer to the Encryption Policy.

Password Policy

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the network.

For more information, please refer to our separate Password Policy.

Removable Media Policy

The removable media policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the company to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following:

- CDs / DVDs
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Card Readers

Security Response Plan Policy

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as a coordinated response in times of crisis (e.g. a security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines.

For more information on policy and procedures relating to security response, please refer to the Security Response Plan Policy.

Development Policy

Before starting development on any project, a data protection impact assessment must be performed and the recommendations added to the requirements of the project.

The requirements for the development must include information security.

Development and testing must be conducted on isolated systems.

All developed systems should undergo security testing at key stages of the project. The results from these tests should then be incorporated back into the project.

Disciplinary action or failure to comply

An employee found to have violated this or any policy stated within the Information Security Management Policy may be subject to disciplinary action.

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