Access Control 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, Monitoring Policy, Password Policy, Acceptable Use Policy
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Access Control Policy			
Description	To define the approaches used to ensure that an appropriate level of security is enforced and maintained to restrict access to these areas, equipment, systems and services.			
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

Purpose

As stated in the Information Security Policy, DE Photo (Franchising) Ltd (referred to as the company here after) shall restrict access to areas, equipment, systems and services to prevent data breaches. This policy states the approaches used to ensure that an appropriate level of security is enforced and maintained to restrict access to these areas, equipment, systems and services.

Scope

This policy applies to all of the company's premises, employees, franchisees, contractors, partners, visitors, third parties, systems, services and equipment. This policy is to apply at all times. It will apply throughout the equipment's lifecycle from acquisition to disposal. Remote and mobile users are also covered by this 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

Definitions

Access control – Rules, systems, and procedures to restrict access to information resources and systems.

Principle of least privilege – Where people are assigned the absolute minimum amount of access necessary to fulfil their role.

Visitor – A third party not under contract that is allowed on the premises.

Suspended – A user account that continues to exist within the system but grants no access.

Unique identifier – A method of identifying something with a unique number or tag such as a serial number.

Roles and responsibilities

All employees and franchisees – Must abide by all clauses of this policy and follow the relevant procedures.

Contractors – Must abide by the restrictions laid out in their contract.

Information Security dept. – Is responsible for making sure that the policy is complied with and making all parties aware of their responsibilities. They must maintain and monitor the security systems.

HR management – Is responsible for informing relevant parties of changes in staff roles or personnel changes

IT administration dept. – Test and maintain systems as instructed by the Information Security Department

Visitors – Must sign-in and be accompanied at all times and must not enter areas marked as restricted.

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

Systems access

Information systems and the networks used to access them must have the appropriate levels of access control. The reasons and approach to securing this information can be found in the Information Security Policy and its supporting policies. All systems including development resources, equipment and devices will need to control access according to the following standards:

- Single systems containing multiple classifications of data will need to have restricted access.
- Access to systems/information/networks should require a formal access request outlined in the access control procedure.
- Users of systems/networks should be issued with a unique identifier and their activity monitored according to the Monitoring Policy.
- Level of access shall be based on the requirements of their duties and responsibilities and adhere to the principle of least privilege.
- All systems/information/networks must be protected with some level of authentication
- Where feasible multifactor authentication should be used.
- Unattended systems/information/networks should not be left logged in.
- Any default authentication settings must be changed.

Users

Users that have access to the information systems and networks need to be aware of their tasks, roles and responsibilities. This should be communicated to them as stated in the training policy and records of this should be kept.

All users should be taking steps to make sure that their user IDs are not used to access information that they are not authorised to access. In order to secure access for users the following standards should be met:

- New users must be created in a way that complies with the User Creation Procedure.
- If a user's role changes their account should be immediately suspended and reviewed to make sure that their access is updated accordingly.
- If a user's account is used in an attempt to circumvent access control the account should be immediately suspended.
- As outlined in the Password Policy and Acceptable Use Policy users should only use their authentication and no one else's.

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

Authentication and authorisation

- Default authentication must be changed before the device/system is in use.
- All authentication for systems, locks, and services must adhere to the company Password Policy.
- Passwords, security PINs and encryption keys should never be re-used
- Password records should be stored in a way that is compliant with the organisation's Password Policy.
- All Passwords should have an expiry date and be changed regularly.

Compliance

Performance Indicators

Incidents where this policy is violated are to be recorded in an incident log and reviewed. Repeated incidents must trigger a review and update of this document. Where an incident is suspected to have led to a breach the breach response plan must be enacted.

Software to monitor access to various systems must be setup on all restricted systems where possible and the systems will need to be regularly tested and result of the monitoring software needs to be regularly reviewed.

Non-compliance

Compliance with this policy is not optional, any employees 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 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