Security Monitoring 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	
Related Material	
Acknowledgements	CYBER123, GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Security Monitoring Policy			
Description	Defines the environment and circumstances under which Network Services, Systems and Data Communications Monitoring activities will be performed			
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
Policy 4
Ethics 4
Network services and applications 5
General 5
Telephony 5
E-Mail 6
Web access 6
Traffic monitoring 7
Active scanning 7
Compliance 8
Compliance Measurement 8
Exceptions 8
Non-Compliance 8
Management and Review 8

Purpose

This policy defines the environment and circumstances under which Network Services, Systems and Data Communications Monitoring activities will be performed, ie:

- Informs users of the extent that network activities, interactions, services, systems and communications methods may be monitored.
- Identifies what personnel may be authorised to perform monitoring functions.
- Highlights the ethics, procedures and safeguards authorised personnel must employ prior to, during and after performing monitoring functions.
- Identifies what information the monitoring processes may gather.
- Identifies how long recorded information may be retained.
- Outlines the purposes 'monitored information' may be used for, including any actions that may follow e.g. anti-virus measures, anti-spam measures, blocking and restricting access.

Monitoring is an essential tool for gathering information, which may be used for a variety of purposes, e.g.

- Capacity planning for expansion.
- Fault investigations and incident handling.
- Conformance testing against other policies.
- Law enforcement requests.

Scope

From a legal perspective the Regulation of Investigatory Powers Act (RIPA) and the companion Telecommunications Regulations 2000, covering lawful business practice and interception of communications, requires that all users of the DE Photo (Franchising) Ltd IT systems be made aware of the following:

Users are hereby informed that their use of the company's data communications infrastructure, services, systems and applications may be monitored by authorised personnel as permitted by UK legislation. UK legislation allows the monitoring of systems and network traffic without consent for legitimate purposes such as:

- Recording evidence of transactions.
- Policing regulatory compliance.
- Detecting criminal or unauthorised use.
- Safeguarding the integrity of the company's IT Infrastructure.

Policy

Authorised personnel may monitor and analyse network services, systems, data, applications and communications of employees, contractors and temporary staff who are using DE Photo (Franchising) Ltd systems or infrastructures.

Mike Moore (the IT decision maker) has the authority to authorise appropriate staff to monitor the communications infrastructure and all supported systems, services and applications.

It will be considered a disciplinary offence for anyone to engage in monitoring activities without proper authorisation or monitor areas out of their responsibility. Furthermore, it is likely that any individual who violates this policy will be breaking the law.

Ethics

Authorised personnel must:

- Respect the privacy of others.
- Not use or disclose information realised in the monitoring process for purposes other than those for which the process was approved.
- Safeguard information collected in the monitoring process.
- Destroy information collected in the monitoring process when it is no longer required.

Network services and applications

General

All networked systems providing network services or applications are monitored where relevant for:

- CPU Active process utilization.
- File storage anomalies, file types and file sizes.
- Licensed software violations.
- Network statistics e.g., peak and average bandwidth utilisation and errors.
- System and security log anomalies.
- Successful access attempts - user account, date/time stamp, session duration.
- Unsuccessful access attempts.
- Unusual network traffic.

This information is used to help determine whether or not DE Photo (Franchising) Ltd systems are operating as intended. Logs and other metrics are retained for as short a period as possible.

DE Photo (Franchising) Ltd reserves the right to examine any file residing on any server or workstation owned by DE Photo (Franchising) Ltd, connected to DE Photo (Franchising) Ltd 's networks or located on DE Photo (Franchising) Ltd premises. This Policy includes DE Photo (Franchising) Ltd owned machines used at home and personal systems that are connected to DE Photo (Franchising) Ltd 's networks.

Telephony

All incoming and outgoing telephone calls through DE Photo (Franchising) Ltd’s telephone systems are subject to the following:

- Call history monitoring
- Accessing call logs and durations
- End to end monitoring of calls dialed and received

Please note if the task dictates it an authorized person may listen and/or record telephone calls or use voice recordings in an ongoing investigation.

E-Mail

All Incoming E-mail processed via DE Photo (Franchising) Ltd mail systems are subject to the following:

- Virus prevention measures, which include blocks resulting from:
- Tests for executable file extensions including bat, exe, vbs etc
- Tests for the initial byte sequence conserved across Microsoft Windows executables
- Signature based anti-virus scanning

Blocking occurs at the SMTP transaction level giving a 'permanent failure' response to the SMTP DATA command.

This approach results in a meaningful error report from their message transport agent (MTA)

Our servers do not compose and deliver 'bogus virus alert' messages to innocent users who have had their e-mail sender details counterfeited

Unauthorised mail relaying is not permitted. This prevents external attempts to use mail systems to relay spam or other messages. Mail from specific sources may be blocked on receipt of valid complaints.

Mail logs are used to follow up problems reported. These logs are kept for [log retention timeframe] then deleted. The length of time that the logs are kept reflects the fact that problems can take some time to come to light if the recipient is absent. field, is held.

Web access

All web access is routed through a firewall.

Cache logs are used primarily to produce statistics on the service. They are also used to investigate any malicious behavior and in the monitoring process.

Traffic monitoring

Authorised personnel may monitor the internet and network connectivity for the following:

- Protocols and applications in use.
- Sources and Destinations - traffic patterns.
- Performance metrics.
- Bytes sent and received per Router and switch interface.
- Errors per Router and switch interface.
- Failure conditions.

Statistical records are retained for as long as they are deemed useful.

Under exceptional circumstances i.e., to help investigate incidents or fault conditions, specific interactions between endpoints may be monitored and recorded for analysis. Records are retained for as long as the incident or fault is active after which time all records are destroyed.

Active scanning

Authorised personnel may perform active scanning of network infrastructure to identify vulnerabilities and or compromised hosts. Authorised personnel must exercise due diligence when performing any scanning activity. Authorised personnel must inform the network and system administrators responsible for the systems on a segment of the planned scan activity and provide the following:

- Schedules including time and duration of scans
- Systems performing the scan (IP addresses)
- Object of the scan ie, vulnerabilities to be tested
- Take reasonable steps to ensure the continued operation or functionality of any system being scanned
- Identify systems with vulnerabilities to the relevant system administrators

Records from active scans will be kept to help identify areas where actions associated with other policies may be required.

Compliance

Compliance Measurement

Compliance to this policy will be audited through various methods, including but not limited to, periodic training, video monitoring, business reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Mike Moore (the IT decision maker) in advance.

Non-Compliance

An employee or Franchise Owner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract.

Management and Review

This document must be reviewed at least every 12 months or earlier if there is a change to systems or if there is a need to update policies due to enhancements in security, software or additions to legislation.

Last Review Date: 16-05-2018
Next Review Date: 16-05-2019