Boundary Device Protection 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	Risk Assessment Procedure, Encryption Policy, Data Protection Policy
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Boundary Device Protection Policy			
Description	Defines essential rules regarding the management and maintenance of firewalls at the company and it applies to all firewalls owned, rented, managed, or otherwise provided to / for the company.			
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) takes information security very seriously in order to help secure networks, firewalls and UTM's where appropriate. Firewalls are an essential component of the company's information systems security infrastructure. Firewalls are defined as security systems that control and restrict network connectivity and network services. This policy defines the essential rules regarding the management and maintenance of firewalls at the company and it applies to all firewalls owned, rented, managed, or otherwise provided to / for the company. As firewalls establish a control point where access controls may be enforced this policy is referenced in the Access Control Policy and the Access Control Procedure.

Scope

This policy applies to all firewalls on the company's networks, whether managed by employees, franchisees or by third parties. Departures from this policy will be permitted only if approved in advance and adequate risk assessments are performed and documented.

In some instances, systems such as routers, telecommunications front ends, or gateways may be functioning as though they are firewalls when they are not formally known as firewalls. All the company's systems acting as firewalls, whether or not they are formally called firewalls must be managed according to the rules defined in this policy. In some instances, this will require that these systems be upgraded so that they support the minimum functionality defined in this policy.

Specific Requirements

Required Documentation

Prior to the deployment of every firewall, a log of and a description of permissible services accompanied by a justification for each, must be documented and stored alongside a suitable risk assessment (refer to the Risk Assessment Procedure).

Permission to enable such paths and services will be granted by the information security dept, only when these paths or services are necessary for important business reasons, and sufficient security measures will be consistently employed.

The conformance of actual firewall deployments to the documentation provided will be periodically checked by the information security department. Any changes to paths or services must go through this same process as described below.

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

Block access by default

Every connectivity path and service that is not specifically permitted by this policy and supporting documents issued by the IT department must be blocked by the company's firewalls.

The list of currently approved paths and services must be documented in firewall audit sheets and distributed to all system administrators by the Information Security dept.

An inventory of all access paths into and out of any company internal networks must be maintained by and approved by the information security dept.

Connecting Multiple Machines

Real-time connections between two or more of the company's computer systems must not be established or enabled unless the Information security dept. has determined that such connections will not breach information security.

In many cases, firewalls or similar intermediate systems must be employed. This requirement applies no matter what the technology employed, including wireless connections, integrated services, VOIP, and any broadband connections. Any connection between an in-house system and any external computer system, or any external computer network or service provider, must be approved in advance by the information technology department and approved by the information security dept.

Regular Testing

Because firewalls provide such an important control measure for the company networks, their strength and proper configuration must be tested on a regular basis.

Where vendor software supports it, this testing must include the use of software agents that automatically check to determine whether firewalls remain configured and running in a manner that is consistent with company security policies and any governing standards that may apply.

This testing process must include consideration of defined configuration parameters, enabled services, permitted connectivity paths, current administrative practices, and adequacy of the deployed security measures.

These tests must include the regular execution of vulnerability identification software and the regular performance of penetration tests. These tests must be performed by a competent party.

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

Logging

All changes to firewall configuration parameters, enabled services, and permitted routes must be logged and be subject to a change control board review.

All suspicious activity that might be an indication of either unauthorised usage or an attempt to compromise security measures also must be logged.

These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

Intrusion Detection

All of the company firewalls must include intrusion detection. Among other potential problems, these intrusion detection systems must detect unauthorised modifications to firewall system files and detect denial of service attacks in progress.

Such intrusion detection systems must also immediately notify technical staff in a position to take corrective action.

All technical staff working on firewalls must be provided with access to systems and privileges so that they can immediately respond to these incidents.

External Connections

All in-bound real-time Internet connections to the company networks or multi-user computer systems must pass through a firewall before users can reach any terminal. No computer system may be attached directly to the Internet unless it is protected by a firewall.

The computer systems requiring firewall protection include web servers, electronic commerce servers, RDS Servers, mail servers and any other device that contains personally identifiable information or proprietary information.

All personal computers with internet connectivity must employ a firewall approved by the information security dept.

Extended User Authentication

Inbound traffic, with the exception of Internet electronic mail, regular news distributions, and push broadcasts previously approved by the information technology department, that accesses the company networks through a firewall must in all instances involve extended user authentication measures approved by the information security dept.

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

Virtual Private Networks (VPN)

To prevent unauthorised disclosure of sensitive and valuable information, all inbound traffic, with the exception of Internet mail and approved news services that accesses the company networks must be encrypted according to the standard defined in the Encryption Policy. The VPNs permissible on the company networks combine extended user authentication functionality with communications encryption functionality.

Firewall Access Mechanisms

All the company firewalls must have unique passwords or other access control mechanisms.

The same password or access control code must not be used on more than one firewall. Whenever supported by the involved firewall vendor, those who administer the company firewalls must have their identity validated through extended user authentication mechanisms.

In certain high security environments designated by the information security dept, such as the company websites, remote access for firewall administrators is prohibited.

All firewall administration activities must take place in person and on site where possible.

Firewall Access Privileges

Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few technically-trained individuals with a business need for these same privileges.

These privileges must be granted only to individuals who are full-time permanent employees of the company or a designated contracted third party IT Supplier, Access must not be granted to temporary staff, contractors, consultants, or outsourced personnel.

All firewalls must have at least two staff members who are adequately trained to make changes, as circumstances require.

Care must be taken to schedule leave time so that at least one person capable of effectively administering the firewall is readily available at all times.

Demilitarised Zones

All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls, and be located within a demilitarised zone (DMZ), a subnet that is protected from the Internet by one or more firewalls. An internal network, such as an intranet, is also protected from the DMZ subnet by one or more firewalls.

Network Management Systems

Firewalls must be configured so that they are visible to internal network management systems. Firewalls also must be configured so that they permit the use of remote automatic auditing tools to be used by authorised the company staff members or contracted third party security companies.

Unless deliberately intended as a test, such automatic auditing tools must not trigger a response sequence through firewall-connected intrusion detection systems or put any production related processing or company, client, or confidential data at risk.

Disclosure of Internal Network Information

The internal system addresses, configurations, products deployed, and related system design information for the company networked computer systems must be restricted such that both systems and users outside the internal network cannot access this information.

Secure Backup

Current off-line back-up copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files, and related files must be kept close to the firewall at all times.

A permissible alternative to offline copies involves encrypted versions of these same files. Where systems software permits it, the automatic reestablishment of approved copies of these systems files must proceed whenever an unauthorised modification to these files has been detected.

Firewall Dedicated Functionality

Firewalls must run on dedicated machines that perform no other service based activity, including but not limited to mail services.

Sensitive or critical company information must never be stored on a firewall. Such information may be held in memory as it passes through a firewall.

Firewalls must have only the bare minimum of operating systems software resident and enabled on them.

Where the supporting operating system permits it, all unnecessary and unused systems software must be removed from firewalls.

The company does not permit its internal information to be resident on or processed by any firewall or server.

Outsourced shared routers, hubs, modems, and other network components that are permissible and approved by the information security dept. must also have relevant risk assessments and documentation.

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

Firewall Change Control

Because they support mission critical information systems, firewalls are considered to be production systems. All changes to the firewall software follow the change request policy.

Update Procedure

The company's firewalls must be running the latest approved and tested release of software/firmware to safeguard against security breaches and attacks. Firewalls and boundary devices are subject to the same update and maintenance plans as any other device or maintained software package within the company.

Firewall Physical Security

All the company's firewalls must be located in locked cabinets or rooms accessible only to those who perform authorised firewall management and maintenance tasks.

The placement of firewalls in an open area within a general purpose data processing centre is prohibited, although placement within separately locked rooms or areas, which themselves are within a general data processing centre is acceptable. These rooms must be equipped with alarms and a log of all persons who gain entry to the room.

Compliance

Monitoring and 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.

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 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 every 6 months unless performance indicators, changes to legislation or the organisation necessitate it.

Last Review Date: 16/05/2018

Next Review Date: 16/01/2019

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