Data Security Policy Document

MK Agents - General structure of this document is based on the headings Purpose, Scope and Policy (Sophos, 2014) (paloalto, 2020).

1.0 Purpose

MK Agents is a company that involves the storage and usage of data about users, properties, financial transactions and other sensitive topics. As well as this, MK Agents has IT resources that are at risk of damage or loss, ranging from desktop computers to network infrastructure.

This document aims to establish a set of policies that protect the data of MK Agents, along with the data of its users, describing policies and tools which are intended to protect from risks.

2.0 Scope

1. This document applies to anyone that:
   a. Utilises company resources including but not limited to desktop computers, landline telephones, mobile telephones and network infrastructure.
   b. Handles or has some level of access to user and company data specific to MK Agents.
   c. Utilises the company's network infrastructure beyond any publicly accessible networks.
2. The data intended to be protected is:
   a. Personal data relating to users.
   b. Data about real estate listings, including addresses and contact information for current occupants.
   c. Financial information.
   d. Other private business data including communications.

(Sophos, 2014)

3.0 Policy

1. Computers and Encryption
   a. Desktop computers and laptops must have full-disk encryption, using BitLocker or Linux Unified Key Setup encryption.
   b. Remote connections must take place through the Company VPN.
   c. Email communication must take place through the standard email client.
   d. Only approved software may be installed onto company computers.
   e. USB devices must be approved before usage.
   f. Any data transferred to external storage must be encrypted to company standards.
   g. Security updates must be completed as soon as they are available before the use of any computers.
   h. Any devices with access to sensitive data must have the ability to be remotely wiped using software.
   i. All computers must be password protected with
2. Employee Requirements
   a. Desks must always be kept tidy.

    b. Employees must not bring in unapproved electronics such as mice or USB sticks.
    c. Any company devices that are lost must be reported immediately to the IT team.
    d. Terminated employees must return all data, records and electronics upon termination.
3. Network Infrastructure
    a. All internal network traffic must pass through a correctly configured hardware firewall.
    b. User data must be stored on encrypted file servers, compliant with the Data Protection Act 2018.
    c. Outward facing servers, such as web servers, must be placed into a demilitarised zone.
4. Physical Security
    a. Any visitors or customers must be escorted when on company premises. Any visitors or customers found without an escort must be escorted off the premises or assigned a new escort.
    b. Server rooms must be restricted to authorised personnel only and be kept locked when not in use.

(Sophos, 2014) (Infosec, 2014)

4.0 Evaluation of Tools

1. Bitlocker
    - Bitlocker is a whole-disk encryption service offered by Microsoft, which has integration with Windows (both desktop and server editions). The service offers recovery keys for devices that can no longer access encrypted volumes, such as with drive swaps or system replacement (ShenLanJohn, et al., 2018). Bitlocker has historically been found to have issues with Solid State drives (Hoffman, 2019), failing to encrypt data securely. Bitlocker is still a strong offering for encryption due to the simplicity and operating-system level integration, alongside the backup keys that are provided.
2. Linux Unified Key Setup (LUKS)
    - LUKS is utilised by many Linux distributions, offering a whole-disk encryption service presented during installation. It’s a comparatively simple encryption service that offers multiple keys and key revocation, without being bogged down with additional features. The reason LUKS is important to consider is that it’s incredibly standard within Linux, while offering a good amount of security. It is lacking some features compared to Bitlocker and some external tools, however the ease of use is reason alone for it to be considered (Guardian Project, 2020).
3. Hardware Firewall
    - This form of firewall is preferable to software firewalls due to a few major features; it’s faster than a software firewall, being specialised hardware, is separate from other hardware such as routers, and has its own software that’s built to a higher security standard. The only disadvantages to a hardware firewall are the costs and physical

space requirements, requiring networking and setup (Anandsoft, 2019).

4. Demilitarised Zone
    - Created using two firewalls, a Demilitarised Zone or DMZ is important when dealing with public facing servers or devices. It allows for less restriction on traffic between the DMZ and the wider internet, with extra restriction between the DMZ, internet and the internal network. While it costs more to set up and requires a specific network topology, DMZ's can be very important in networks due to the multiple layers of security that help prevent infections to the whole network (Barracuda, n.d.).

5.0 References

Anandsoft, 2019. *Advantages and Disadvantages of Hardware Firewalls..* [Online]

Available at: https://www.anandsoft.com/networking/advantages-of-hardware-firewalls.html
[Accessed 8th January 2020].

Guardian Project, 2020. *LUKS: Disk Encryption.* [Online]
Available at: https://guardianproject.info/archive/luks/
[Accessed 8th January 2020].

Hoffman, C., 2019. *You Can't Trust BitLocker to Encrypt Your SSD on Windows 10.* [Online]
Available at: https://www.ru.nl/english/news-agenda/news/vm/icis/cyber-security/2018/radboud-university-researchers-discover-security/
[Accessed 8th January 2020].

Infosec, 2014. *IT Security Policies Should Include a Physical Security Policy.* [Online]
Available at: https://resources.infosecinstitute.com/security-policies-include-physical-security-policy/
[Accessed 8th January 2020].

paloalto, 2020. *What is an IT Security Policy?.* [Online]
Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy
[Accessed 8th January 2020].

ShenLanJohn, et al., 2018. *BitLocker.* [Online]
Available at: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
[Accessed 8th January 2020].

Sophos, 2014. *Sample Data Security Policies.* [Online]
Available at: https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en
[Accessed 8th January 2020].