Network Security Policy

Policy Brief and Purpose

This network security policy clearly states the rules and guidelines that must be adhered to when using the network with any device at any point. The purpose of these rules and guidelines is to protect the information assets owned by the company which are provided by its computers and smart devices on the network. Protecting these assets adhering to the policy will prevent unnecessary breaches from attackers, human errors and system malfunctions on the network. As an employee of the company you are solely responsible for maintaining that your devices on the network adhere to these rules and maintain the confidentiality, availability and integrity of the network for all its users. Further noting that if you think you may have disobeyed one of the instructions and caused potential damage please contact the network administrator immediately. Please note that if you do not understand any terms or seek further clarity then check the definitions and terms section at the bottom of the document.

This security policy should be distributed to all members on the network regardless of their role in the company. If you require an altered version of this policy for any reason please contact the network administrator directly and state why, a suitable copy will be distributed to you. All employees of the company must make every effort to comprehend and comply with the policy.

Scope

The scope of this policy covers all employees of the company, whether that be permanent or on a temporary basis, this further includes contractors, consultants and volunteers that are personally affiliated through third parties if they own or use a device that is part of the company’s network. The scope also covers all possible devices that are used on the network, this includes any endpoint device that is or was connected to the company network or using the company site. These devices include computers, laptops, phones, tablets and any ‘thing’ that can transmit a data packet wired or wirelessly across the network.

Policy

General network requirements

* Minimise the transfer of sensitive data if possible.
* When transferring large volumes of sensitive data seek the network administrators help.
* Only share confidential/sensitive data over the company’s network.
* Do not share confidential/sensitive data over a public connection.
* All employees must report any suspicious network activity to the network administrator. This includes and is not limited to, hacking attempts, privacy breaches, malware and phishing scams.
* Do not write passwords down physically.
* Change password every season.
* Do not leave any device unattended in or outside the company.
* Do not log into the company’s network through an insecure port or another person’s device.
* Devices connected to the network must be locked and screens turned off when not in use.
* Report damaged or faulty software/hardware to the IT department as soon as possible.
* Report any possible weak points in the networks security if it becomes noticed.
* Do not download any content from untrusted sites.
* Do not download or browse untrusted sites during your break.
* All employees should not have access to the network until they comprehended and complied to the policy
* All employees must complete mandatory network security training.

General device requirements: This includes any wireless device connected to the company’s network or provides confidential information relating to the company.

* Must use an appropriate authentication protocol. (PEAP or EAP-TLS)
* Must use an appropriate encryption protocol. (TKIP or AES)
* Bluetooth devices must be encrypted with SSP.
* Wired devices must be connected using company provided ethernet cables.
* All devices must be connected to the network by an approved and qualified employee.
* All devices must be supported and maintained on the network by an approved and qualified employee.
* All devices must have a trackable MAC address.
* All devices MAC addresses must be registered and stored by the company.
* All devices must not interfere with the networks wireless access points.
* All devices must be password protected. (8 characters with upper and lower case)
* All devices must have an adequate antivirus software.
* All devices must be kept up to date.
* Do not lend your devices to another employee.
* If any issues occur speak to the network administrator, not a fellow employee.

Home Wireless device requirements

* All devices that have direct access to the company’s network must be first approved by the company’s network administrator.
* All devices that have been approved onto the network must follow the general device requirements as stated above.
* All devices must use standard remote access authentication when connecting to the company network.
* All devices should only connect to the company network if permitted by the administrator.
* Devices must have WPA-PSK.
* Make sure the pre shared secret key is complex (minimum 15 characters)
* Do not broadcast your SSID.
* Do not stay logged in to the company network from home if you are not present at home.

Program Requirements

* When opening and using the program ensure that no other programs are running.
* Ensure that there is no one present when running the program that could use the information maliciously.
* Ensure that whoever is using the program has been trained to do so.
* Ensure that the user has clearly read and comprehended the guidance document.
* Ensure that the encrypted documents password is strong. (8 characters with upper- and lower-case minimum.)
* Ensure that the password is not written down physically.
* Ensure that the password is changed every 2 months.
* Ensure an anti-virus software is running when using the program.
* Close the program once finished using it.
* Don’t leave the program running unattended.

Future ‘things’ requirements

The future of technologies and networks within cyberspace is ever-growing, with the number of connected “things” increasing as well as the data that is transmitted through them. Traditional security solutions will not be able to stop cyber-attacks in the future, therefore future considerations create policies and software’s to protect against attacks in the future (Managementevents.com, 2018). The rise in Internet of Things devices being used in businesses and organisations has seen security and privacy concerns rising, this is due to the issue that “things” can be connected to the internet or to another “thing” with extreme ease. This creates large networks and bigger attack surfaces meaning that it is less secure.

* Analytical and automated security integration approach; helps to build an analytical model that is capable of detecting and fixing flaws before a cyber-attack can happen (Managementevents.com, 2018). Include intrusion detection systems, security monitoring and scanning for vulnerabilities; using security automation allows for the execution of security operation without human intervention (Humphries, 2019).
* Blockchain; with cyber attackers often targeting valuable data such as financial transactions, personal information, bank details or health records. Majority of Internet of Things devices hold valuable and private information either on a mobile phone or secure network connections. Blockchain provides a transactional data structure that is encrypted, transparent and irreversible, which means there is not a hackable gap for attackers to take control of the network (Managementevents.com, 2018).
* Artificial intelligence; has many benefits to businesses and organisations cybersecurity such as attack detection and natural language processing. The use of machine learning algorithms artificial intelligence will be able to improve the ability to detect any potential attacks. Artificial intelligence can also improve password protection by monitoring how passwords are created (Davis, 2019).
* Security by design; perform risk analysis involving cybersecurity specialists from early stage of design process of device in order to find out which security features will be required.
* Privacy by design; this should be applied from the first stages of network development. Separate data that could be used to identify an individual from other information and ensure it is encrypted.
* Risk and threat management; perform a risk analysis annually, it should include technical and procedural testing of the effectiveness of the security policies in place.
* Machine to Machine security; measures regarding encryption and communications, establish a security connection with secure cryptographic algorithms between the communicating units to provide authentication, integrity and confidentiality.
* Incident handling; detection and response to incidents that may occur. Establish a process for incidents that consists of identification of affected resources and detect and investigate promptly every unusual security related event.

References

Davis, M. (2019). How Artificial Intelligence is Shaping the Future of Cybersecurity - AXEL Blog. [online] AXEL Blog. Available at: https://www.axel.org/blog/how-artificial-intelligence-is-shaping-the-future-of-cybersecurity/ [Accessed 3 Jan. 2020].

Enisa (2018). Good Practices for Security of Internet of Things in the context of Smart Manufacturing. Maroussi: Enisa, pp.37-45.

Managementevents.com (2018). 4 Key Areas Shaping the Future of Cyber Security | News. [online] Managementevents.com. Available at: https://managementevents.com/news/4-key-areas-shaping-the-future-of-cyber-security/ [Accessed 3 Jan. 2020].

Manager, S., Humphries, S., Humphries, S., Daughney, T., Daughney, T., Cassetto, O. and Cassetto, O. (2019). Beat Cyber Threats with Security Automation. [online] Exabeam. Available at: https://www.exabeam.com/incident-response/security-automation/ [Accessed 3 Jan. 2020].

Policy Compliance

In order to maintain the compliance and comprehension of the policy all employees must sign a contract stating so. This contract allows all users of the network and its devices to have the policy enforced upon them. All users of the network will be made subject to random policy enforcement checks. These checks can include internal and external audits, device and network monitoring and walk throughs. Failure to comply with the policy will result in the following outcomes:

Minor incidents – breaking or ignoring the policy without causing any damage to the network or its devices results in mandatory completion of further security training followed by a verbal warning.

Major incidents – breaking or ignoring the policy resulting in damage to the networks confidentiality, integrity and availability on a large scale, therefore requiring advanced disciplinary action up to and including termination.

Exceptions – the network administrator may wish to provide exceptions to some rules if they are deemed to be outdated, disciplinary action will therefore be dropped.