PANGEOTEK

IT & SYSTEMS HARDENING POLICY

IT POLICY

INTRODUCTION

In today's digital age, technology plays a vital role in the success of any organization. As a small business, it is important for us to ensure that our IT systems are secure, efficient, and aligned with our business goals.

The purpose of this policy is to ensure the security, reliability, and confidentiality of the company's IT systems, as well as protect the intellectual property, personal data, and confidential information of both the company and its customers

This policy outlines the guidelines and procedures for the use of IT resources within our organization. It is designed to protect our confidential information, ensure compliance with legal and regulatory requirements, and promote productivity and innovation. By adhering to this policy, we can ensure that our technology supports our business objectives and helps us to achieve our goals.

POLICY

- All employees must follow the company's standard security procedures when accessing company information or systems. This includes using strong passwords and keeping them confidential, logging off when leaving a computer unattended and being vigilant for any suspicious activity.

- The company's information and systems are confidential and must not be shared or disclosed to unauthorized individuals.

- Employees must comply with all data protection and privacy laws and regulations.

- All software installed on company computers must be licensed and must be used in accordance with the license agreement.

- Regular backups of important company data must be performed and stored in a secure location. Backups should be held in Cloud based storage. Any data that is held/backed up onto physical drives should be encrypted and stored in a safe location so that it can not be accessed by unauthorised persons.

- All employees must ensure that their work is saved to the appropriate network location.

- The company's computers and networks should be monitored for security threats and appropriate action must be taken to protect the company's information and systems.

- Employees should use caution when accessing the internet, as malicious software and websites may be present.

- All Passwords must be strong and changed regularly.

- Company computers must be used in accordance with all applicable laws and regulations.

- Physical access to company computers must be restricted to authorized personnel only.

SYSTEMS HARDENING POLICY

INTRODUCTION

System hardening is a process of making systems less vulnerable to attack and more reliable. It is done by changing how the system is configured, installing security updates and patches, and using firewalls. In a small business setting, hardening your systems is crucial in order to protect sensitive information and ensure the continuity of your operations.

Pangeotek recognise that small businesses face unique challenges when it comes to systems hardening. Some of these challenges include a lack of resources, a need to keep operations affordable, and the need to maintain a flexible and fast-moving business.

We understand that in order to help our businesses succeed in systems hardening, it is important to have a policy in place that outlines the steps that will be taken to protect the business. By adhering to this policy Pangeotek can greatly reduce the risk of cyber attacks and other security incidents. Some of the measures required for systems hardening are also part of our IT Policy.

POLICY

Pangeotek ensure that the following measures are in place to protect their systems:

- **Use of a Firewall and VPN**: Ensure that a suitable firewall is installed and regularly updated to protect the system from malicious threats. Pangeotek's Senior Consultant uses NordVPN on his mobile phone and laptop. Nord VPN is a virtual private network (VPN) service that offers a range of features, including military-grade encryption, cyber security, and double VPN technology. It also provides access to over 5,000 servers in 59 countries, allowing users to access content from around the world.

- **Install Antivirus Software**: Install a reliable antivirus software to protect the system from malware and other malicious threats. Ensure that the antivirus software is set to automatically download and install updates as soon as they are available.

- **Update Software Regularly**: Ensure that the operating system and other software installed on the computer are up to date. Check that updates are from a genuine source.

- **Disable Unused Services**: Disable any unnecessary services or applications that are not needed for the system to run.

- **Set Up User Accounts**: Set up user accounts with strong passwords and only allow access to those users who need it.

- **Monitor System Logs**: Monitor system logs to ensure that any suspicious activity is detected and dealt with quickly.

- **Back Up Data:** Back up data regularly to ensure that any lost data can be recovered. This should be done onto a local drive as well as onto Cloud based storage.

Lee White
Director/Senior Consultant
Pangeotek Ltd

Last Reviewed 26th May 2023