***A picture containing graphics, graphic design, logo, font

Description automatically generated***

***TechBros Security Policy***

1. **Introduction**

This Security Policy (SP) for TechBros Assets is designed to protect TechBros assets from any threats that can be opposed on the company assets. This policy is used to protect our employees, customers, and other partners from any effect that the different threats can have on the specific asset. Threats can be both deliberate and inadvertent action.

The aftermath of these threats can be severe. Potential damage includes but not limited: loss of data, loss of revenue, network destruction and other more damages.

Everyone who works at TechBros is responsible for the security and safety of the assets. As such, all employees must ensure they always adhere to the guidelines in this policy. Should any employee be unclear about the policy or how it impacts their role should speak their management or the IT department.

1. **Definitions**

**An asset** is any item such as data, device or any other type of components that is found out through the environment that supports the normal functioning of the company activities.

**A threat** is defined as any situations or incidents with the potential to negatively affect the normal functioning of different sections (assets, operations and individual) of an organization through a system through different ways such as unauthorized access, destruction and more.

1. **Scope**

This is a universal policy that all applies to all the assets that the TechBros owns or borrow from other companies. For some assets and/or some assets a more specific policy exists in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply to other points.

The policy covers all the TechBros assets. Staff members at TechBros who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with guidelines and rules.

1. **Assets**

All assets that are stored on TechBros is the property of TechBros. Individuals should be aware that the company cannot guarantee what are the effects that the different threats can have on these assets owned by TechBros.

Throughout different location or departments of TechBros, these assets are used in the normal functioning of the company. These assets include but may not be limited to computers, servers, routers, WhenToWork, and more.

TechBros assets is any component that is found throughout the environment is used in the normal functioning of the company. These assets should be used on property and never be used outside of the property expect from permissions from management. However, it must not be in any way detrimental to users own or their colleague’s productivity.

In certain events, personal usage of assets may be allowed, if this will neither prevent the Company from implementation of its tasks and activities, nor infringe the legality of Company's activities; assets may not be used to gain personal benefits or for any other improper purposes, or otherwise violate this Policy and other policies of the Company.

TechBros trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company’s assets. If employees are uncertain, they should consult their manager.

TechBros can monitor their assets by doing an assets identification assessment for their company.

TechBros reserves the right to regularly audits of their assets to ensure compliance with this policy.

A close-up of a document

Description automatically generated

1. **Threats**

In any given day, TechBros assets are faced with different threats that can affect the normal functioning of the company. Individuals should be aware that these the company can’t guarantee when will these threats will happen and the aftermath of these threats happening. Threats can be both deliberate and inadvertent action.

The company can only give a hypnotical estimate probability of these threats happening. These estimate probabilities are found out through a threat identification assessment of different threats that the company can faces.

There are many different threats that can be performed to affect the normal functioning of TechBros. This includes but is not limited to: Forces of Nature, Deliberate Software’s Attack, Espionage, Deliberate Acts of Thefts and more. The different assets that are used throughout the company faces different vulnerabilities such as olde versions, less/no security which leads threats easily to be performed on these assets.

TechBros trust employees to be fair and report if theses threats are being performed on these assets. And report the different effects that these threats can have on TechBros assessment.

A close-up of a document

Description automatically generated

A close-up of a paper

Description automatically generated

1. **Threats Prevention**

After a threat is performed on the Company, the aftermath effect on the company can be serve or non-severe. Some effects that’s these threats can have on the company includes but not limited to loss of data, loss of revenue, network destruction and more.

When the process of identifying and analyzing the effects of the different effects of these threats on the company, different migration strategies should be performed to prevent these threats on these the company assets.

TechBros has a set of rules and regulations when it comes with the recovery of different threats on their company assets.

A screenshot of a computer screen

Description automatically generated

1. **Rules/Guidelines**
2. Use company resources responsibly to ensure that they are misused or wasted.
3. Be attentive to security procedures and be alert for situations that may lead to loss, theft, or misuse of resources. All employees must report all situation to management.
4. Do Bi-weekly training to ensure all security produces is practiced and learned.
5. Devices connected to the network must comply with the minimum access policy.
6. The Company's information technology system, telephones and other technology resources may be used only for legitimate business-related communications, though occasional incidental personal use that is professional and does not interfere with the Company's business may be permitted with written approval from proper management.