Information Technology Policy

This policy applies to employees, contractors, consultants, temporary and other workers at Engenuity Solutions, including any third parties, to all information assets owned or leased to Engenuity Solutions or any devices connected to Engenuity Solution's network. These information assets must not be used in an unlawful or unethical way. Workes are responsible for using all information assets in compliance with the company policies and guidelines.

Engenuity Solutions do not assume any responsibility if employee devices are infected by malicious software or if their data are compromised due to inappropriate employee use.

Internet and E-mail usage

Employees are permitted to use Engenuity Solutions' company internet connection for the following reasons;

- To complete their job duties
- To seek out information that they can use to improve their work

Employees are to exercise sound judgement and remain productive at work while using the internet. Any use of our network and connection must follow confidentiality, and employees should;

- Keep their passwords secure at all times
- Log into their corporate accounts only from safety devices.
- Use strong passwords to log into work-related websites and services.

Employees can use their corporate email accounts for both work-related and personal purposes if they do not violate the policy's guidelines. Employees should not use their corporate email to;

- Register to illegal, unsafe or disreputable websites and services,
- Send obscene or offensive messages and content.
- Send unauthorised attachments or solicitation emails.
- Use reasonable caution when opening email attachments or links.
- Take care when forwarding emails.

Employees must not use the network to;

- Download or upload obscene or illegal material.
- Send confidential information to unauthorised recipients.
- Invade another persons' privacy and sensitive information.
- Download or upload movies, music and other copyrighted material.
- Visit potentially dangerous websites that compromise the safety of our network and computers.
- Perform unauthorised or illegal actions.

We advise employees to be careful when downloading and opening/executing files and software.

Computer Virus Protection Policy and Acceptable Computer Device

This Policy dictates the use of anti-virus software on any device attached to the Engenuity Solutions network and storage drives. It addresses acceptable virus protection software and the frequency of scans. This Policy applies to any device connected to the ES network, including but not limited to computers, mobile phones, and tablets.

- Maintain recently updated version of an operating system, e.g., Microsoft 10, Linux, macOS.
- Maintain an anti-virus program installed on all connected devices. It should be configured in a real-time protection configuration.
- Maintain virus definitions through updates at least once a week.
- Virus scans should be completed at least once a week.

All users must be aware of how their systems and subsequently the company's systems can be infected. Users must be cautious when opening emails, email attachments, unknown files, and when accessing the internet.

- Users should know what file types they are accessing and have their systems configured to show file extensions.
- Users should only open attachments from reputable sources.
- Users should be aware of the way that email addresses can be spoofed to look like reliable senders.
- Users should be vigilant of any website posing as a reliable source.
- Any potential issue should be reported to their supervisor.