CROWBERRY CONSULTING

Environment, Ethics and Corporate Responsibility Management

Cyber Essentials Policy

Firewalls

Only firewall rules that are necessary for the running of the business are allowed and must be approved by 127 Solutions. Any open ports that are no longer required will be disabled as soon as they are no longer needed.

Default Deny Policy

If a system has no requirement for internet access, then this system will be denied access to the Internet.

Backup Policy

Automated daily backups are in place to secure data. These are monitored on a daily basis to ensure completion. A designated user on site must swap the backup media before the end of each day and take the most recent backup off site to secure the data.

Password Policy

Passwords must be reset every 60 days by all users. These must consist of at least one uppercase and one lower case letter, one wild card character, one number and contain at least eight characters. Using repeat passwords and sequential passwords is not allowed.

Malware Protection Policy

Malware protection software must be kept up to date with a valid subscription at all times. Schedules are in place to make sure that the Eset Smart Security software checks for engine updates through the day and applies them automatically. The software must not be disabled at any time.

Mobile Working Policy (BYOD)

Any BYOD devices that are used in the workplace must have all vendor software updates and patches installed before they are given access to the Wi-Fi network. Any devices that are not up to date will be denied access to the network.

Becky Toal
Managing Director
V001/19/08/2015