IT Security Policy Statement

WCS Group is committed to protecting the company's employees, properties, information, reputation and customer's assets from potential threats. An IT Security Policy is needed to help satisfy and deliver on this commitment safeguarding both the company and customer's ability to operate safely, reliably and without catastrophic interruption or significant risk.

This Policy is guided by the company's basic core values, code of conduct, business ethics and supply chain security standards, and it fashions the way the company operates both day to day and across the supply chain. All security activities must adhere to the general principles laid down below.

Scope

This Policy affects all company employees – particularly but not limited to those with responsibility for data security. It covers security arrangements for the protection of core business infrastructure assets and data held on computers, servers located on sites owned by the company in the event of fire, hacking or an adverse event which could affect the data, integrity of data, accessibility or storage. It extends to the protection of IT assets owned by the company whilst in the possession of employees off site or at home or travelling between home and work. Its prime purpose is to show that data cannot easily be lost, stolen, destroyed or corrupted.

Responsibility

The Senior IT Manager is responsible for overseeing the backup data procedure, including the appointment of a deputy to undertake related duties. The Senior IT Manager or deputy must ensure the basic backup disk is changed daily and data for the last 24 hours is removed from site. A replacement back up disc must be used from the fire safe located in the Communication room.

It is the responsibility of Team Metalogic, the outsourced incumbent IT service provider, to maintain the computer hardware and data access of WCS Group.

Policy

Data storage and backup

- All core business data is held on servers in a secure communications room in the Head Office
- Servers are backed up overnight on a 5-day backup schedule using shadow copies, stored locally at twice-daily intervals (07.00 and 12.00hrs) enabling documents to be 'rolled back' to a previous state. The latest backup cartridge is always kept off site.
- Remote servers are located in satellite offices containing site-specific data which is backed up on a 5-day backup schedule, with the latest backup cartridge always kept off site or in a fire-proof safe
- All sites are protected by hardware firewalls and inter-linked via an encrypted hardware VPN, for which is there is redundancy in the event of communication failures

Adverse events and protection

- In the event of a major systems outrage (MSO) at the company's headquarters, remote servers can be elevated to provide authentication and maintain the network infrastructure during the outage
- In the event of a mail-server failure, an in-the-cloud spooling service will hold in-bound emails until such time that they can be (a) delivered to the mail server, (b) redirected to an alternative mail server, (c) read or actioned via a web-based console

- An in-the-cloud spam filtering service prevents known junk-email from being delivered to the mail server, quarantines suspected junk email and removes virus and other malware from email messages prior to delivery to WCS Group mail servers
- A web filtering service prevents access to malicious websites as well as those sites that are deemed unfit or unnecessary for particular employees' job function
- All servers and end-user workstations are protected with a centrally-managed enterprise-grade anti-virus solution, with updates deployed at 3-hour intervals
- The network is considered secure, with non-WCS Group endpoints connecting to guest networks only (there is a guest WI-FI at each site within the corporate network)
- There are no shared user accounts. Each user has an assigned username and password
- All users have standard user rights with no local administrative access to their workstations, thereby preventing unauthorised changes
- There is a pre-set process / procedure for the addition of new users and similarly for the removal of users when no-longer employed by the company
- ~Password policies are enforced, requiring a change in password every 90 days. Complexity requirements are also in effect, requiring at least an 8-character password with combination of uppercase, lowercase, numeric and special characters. 24 passwords are remembered by the server, preventing the same password from being re-used
- Permissions are group-based with every user falling in to one or more of 51 available security groups. Permission changes are authorised by the relevant department / line manager and audited fully with users having access only to the data / information they require in order to complete their job function.

Other relevant / related policies:

Quality Policy
Corporate and Social Responsibility Policy
Ethics (Business and Social) Policy
Social Media Policy
Business Continuity Policy
Sustainability Policy
Health and ~Safety Policy
Equal Opportunities Policy
Diversity Equality Employment Policy

Mike Sullivan CBiol., MSB, MWM Soc
Managing Director