WILCOCK CONSULTING
Services to the Onshore Natural Gas Industry

Unit 9
Trinity Enterprise Centre
Furness Business Park
Barrow-in-Furness
Cumbria LA14 2PN
United Kingdom

Tel: +44 (0)1229 824034
Web site: www.wilcock.co.uk

Cyber Protection Policy

Information is a key asset to our clients and its correct handling is vital to the delivery of our services and the integrity of Wilcocks. We are committed to complying with our legal and regulatory obligations and client requirements in respect of information security and to achieving the right balance between the need to share information and the risks associated with security breaches. The security controls below describe how we protect our business.

Office Firewalls and Internet Gateways

- The default password is changed on all routers and firewalls, including those that come with a unique password pre-configured (i.e. BT Hub). This is done automatically by the IT Consultant on set up.
- The new password on all internet routers or hardware firewall devices is at least 8 characters in length and difficult to guess. A password that is difficult to guess will be unique and not be made up of common or predictable words such as "password" or "admin", or include predictable number sequences such as "12345".
- Passwords are changed if it is believed that the password has been compromised for example passwords may be compromised if there has been a virus on the system or if the manufacturer notifies us of a security weakness in their product.
- Where we need to access any software service from outside the office network, this is only performed using an off the shelf tool such as LogMeIn, TeamViewer and VNC which do not require any extra ports to be opened on the firewall (beyond the standard 80 and 443).
- For services enabled on our firewall, we have a process to ensure they are disabled in a timely manner when they are no longer required. If we no longer need a service to be enabled on our firewall, we remove it to reduce the risk of compromise.
- We have configured our internet routers or hardware firewall devices so that they block all other services from being advertised to the internet.
- Our internet routers or hardware firewalls are configured not to allow access to their configuration settings over the internet.
- The access to the settings is protected by either two-factor authentication or by only allowing trusted IP addresses to access the settings.
- We have software firewalls enabled on all of our computers and laptops.

Secure Configuration

- Where we are able to do so, we remove or disable all the software that we do not use on our laptops, computers, servers, tablets and mobile phones.
- We change the default password for all user and administrator accounts on all our laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more.
- All our users and administrators use passwords of at least 8 characters.
- We do not run software that provides sensitive or critical information (that shouldn't be made public) to external users across the internet.
- “Auto-run" or "auto-play" is disabled on all of our systems.

Software Patching

- All **operating systems** and **firmware** on our devices are supported by a supplier that produces regular fixes for any security problems.
- All **applications** on our devices are supported by a supplier that produces regular fixes for any security problems.
- All high-risk or critical security updates for operating systems and firmware are installed within 14 days of release.
- All high-risk or critical security updates for applications (including any associated files and any plugins such as Adobe Flash) are installed within 14 days of release.
- We have removed any applications on our devices that are no longer supported and no longer receive regular fixes for security problems.

User Accounts

- We ensure that user accounts (such as logins to laptops and accounts on servers) are only provided after they have been approved by a person with a leadership role in the business.
- We ensure that staff can only access laptops, computers and servers in our organisation (and the applications they contain) by entering a unique user name and password.
- We have a recorded user access registration and de-registration procedure in place for granting and revoking access to systems.
- We ensure that we have deleted, or disabled, any accounts for staff who are no longer with our organisation.
- We ensure that staff only have the privileges that they need to do their current job.

Administrative Accounts

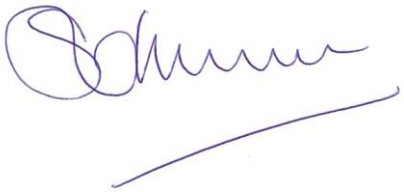
- We have a formal process that we follow when deciding to give someone access to systems at administrator level. This process includes approval by a person who is an owner/director/trustee/partner of the organisation.
- We ensure that administrator accounts are only used when absolutely necessary, such as when installing software. We acknowledge that using administrator accounts all-day-long exposes the device to compromise by malware.
- We ensure that administrator accounts are not used to access websites or download email. Using such accounts in this way exposes the device to compromise by malware. This is achieved through good policy and procedure as well as regular training for staff.
- We review the list of people with administrator access regularly. Any users who no longer need administrative access to carry out their role have it removed promptly.

Malware Protection

- All of our computers, laptops, tablets and mobile phones are protected from malware by: Having anti-malware software installed and /or limiting the installation of applications to an approved set.
- Where we have anti-malware software installed it is set to update daily and scan files automatically upon access.
- Where we have anti-malware software installed it is set to scan web pages we visit and warn us about accessing malicious websites.
- Where we use an app-store or application signing users are restricted from installing unsigned applications.
- Where we use an app-store or application signing we ensure that users only install applications that have been approved by our organisation and we document this list of approved applications.

This policy, and compliance with this policy, will be reviewed at least every twelve months as part of the annual management review in accordance with the quality management system, or more frequently on an ad hoc basis, where required by the Managing Director. Current copies of the policy are displayed in the offices and are issued to all head office employees and the policy is drawn to their attention during their company induction.

This plan is displayed in the Wilcock office, is subject to trial or simulation on an annual basis and is also reviewed annually as part of the overall company Management Review.



Graham Wilcock
Managing Director
22nd September 2021

Rev. 4

Certificate Number 2456 Certificate Number 2456 Certificate Number 2456