CUSTOMER FAIR USAGE POLICY

ATLAS CLOUD

SUMMARY

This policy provides standards for correct and proper use of our Customer's IT networks to protect against degradation of performance and interruption to IT dependant business activities, loss of confidential and business critical information and safely and correctly operating IT equipment.

INTRODUCTION AND SCOPE

The Customer's IT networks are key to the on-going operations of their businesses; incorrect function of these networks would impact on the service provided to their Customers and also profitability.

Furthermore, our Customers wish to protect against loss of data which impacts on the day to day activities of the business, or if disclosed to certain parties, may affect the competitive activities of the business. Certain precautions must be taken to protect against disclosure or loss of information assets.

Finally, as with all electronic equipment, IT hardware can be dangerous when operated incorrectly or in the incorrect environment. It must also be used according to manufacturer's instructions to prevent damage to the equipment.

POLICY

1. PC USAGE

IT hardware can easily be damaged when used inappropriately causing interruption to users and hence the business whilst repairs are carried out or a replacement sourced. Data loss, which may be more damaging to the business, could also occur. Finally, as with any electronic equipment, PCs and related accessories can be dangerous when handled inappropriately or in the wrong environment and it is the duty of the operators to ensure responsible usage.

- Desktops, laptops, workstations (PCs) and related equipment should only be used in the manner and environment described in the applicable user guides and instructions.
- PCs should only be used with recommended peripherals and should not be modified in any way which may invalidate the manufacturer warranty.
- PCs should only be used for business activities or personal activities where specifically allowed by the Customer's own IT policy.

2. HOUSEKEEPING

IT networks have a finite capacity for file and email storage and a certain amount of 'housekeeping' should be practiced by individual users to ensure reasonable storage availability and to prevent impact on performance. Furthermore, storing files in certain areas of a networked computer's file system can impact performance and these practices should be avoided:

- Duplicate files in both users' home drives and on shared drives should be avoided
- Large programme files, audio files or videos should not be stored on the corporate network unless specifically required for business activities
- Junk or expired emails should be deleted from users' email inboxes
- Emails with large attachments should be deleted from users' email inboxes. Where the attachments are required for business purposes, they should be saved to a shared drive
- Files or folders should not be stored on your desktop. Desktop shortcuts to files and folders elsewhere are however acceptable.
- Certain software which stores information in inappropriate locations (examples include iTunes and Google Earth) should not be installed. Where required for business purposes, this software should be installed by an IT administrator (normally the Supplier)
- Running email archiving routines from Microsoft Outlook should be avoided. Where required for business purposes, a dedicated email archiving system should be installed. This software would be installed by an IT administrator (normally the Supplier) and would normally require purchasing.IT hardware can easily be damaged when used inappropriately causing interruption to users and hence the business whilst repairs are carried out or a replacement sourced. Data loss, which may be moOur Terms of Use http://www.atlascloud.co.uk/terms/ also apply to your use of our services.

3. INTERNET AND EMAIL USAGE

Traffic coming from outside the business is the main source of software threats to corporate networks. Almost all software threats including viruses, spyware, trojans and other malicious software are spread through email and the internet and responsible use by operators is therefore paramount to the security of the network.

Antivirus, anti-spam and other network security software will protect against these threats to some extent but will not be able to identify all malicious software. Users should follow best practices to provide a better level of protection against infection.

- Emails from unknown senders with attachments should not be opened and immediately deleted.
- Where an email is received from an unknown sender and it has a link in the email to a website, do not click on the link.
- Where an email is received from a known sender and it has a link in the email to a website, do not click on the link. Instead of clicking on the link, open up Internet Explorer and type in the address that the link says it opens. It is possible for a link in an email to look like it is going to take you to one website, but the actual link that you click on may take you to a different website which may not be safe.
- Do not download and install any software from the internet without consulting your network administrator (normally the Supplier). Internet based software can often contain viruses, spyware and trojans even if they do appear to come from a reputable source.
- Do not engage in any file sharing or other peer to peer sharing activities. This will use up network bandwidth (affecting other users) and files downloaded through these mediums cannot be verified and may contain threats to the network.
- Beware of websites informing you of security problems on your PC. This can be 'scareware' where malicious software is installed and a fee demanded to allow normal functioning of your PC. Any such occurrence should be reported to your network administrator (normally the Supplier).
- Do not visit any websites containing pornographic material, illegal software or those associated with criminal activities. Use of all such websites carries a high risk of introducing malicious software to the network.

4. NETWORK SECURITY AND MANAGEMENT

To ensure proper functioning of corporate IT systems, correct operation of networking equipment is required. Misuse and negligence can result in a reduction in or total loss of IT network functionality and significantly interrupting business activities.

- Do not plug any network devices in without consulting your network administrator (normally the Supplier). This can include switches, routers, wireless access points, printers and scanners.

- Do not remove, replace or add any network cables from the office or from the comms or server areas without consulting your network administrator (normally the Supplier).
- Do not tamper with, power off or remove any network switches. Reasonable precautions should also be taken to prevent to prevent other parties (ie. cleaners) from interfering with this equipment.

5. NETWORK SERVERS

Administration of network servers should be left to your network administrator (normally the Supplier) and they should be in no way tampered with or logged on to by non-qualified users. The server environment should also be kept clean and at temperature of 20 degrees centigrade or below.

6. USER ACCESS AND MANAGEMENT

Correct management of user access is essential in preventing unauthorised persons from having access to your network and your business' data. Unauthorised users can be people from outside of the business, former employees or current employees without the required permissions. All such access, whether malicious or otherwise, can cause damage to the network and interruption to the business. User access and management must therefore be tightly regulated.

- Network users should use a strong password for network access. A strong password should be a minimum of 8 digits, contain letters, numbers and symbols. You should also change your password on a regular basis – once a month is good practise.
- Never leave your PC logged in at the end of the day or for extended periods away from the office and where possible power it off at the end of the working day.
- Addition of new users to the network, and modification to security permissions of existing users, should only be performed by a qualified network administrator. This would normally be the Supplier as your network support provider.
- Users who are no longer required on the network should be disabled and deleted by a qualified network administrator. This would normally be the Supplier as your network support provider. You should notify your network administrator as soon as the user leaves your business.

- Network master administrator passwords should not be disclosed to employees and should be kept off site in a safe or safety deposit box. IT administrators should access the network through individual administrator accounts.