

The Visual Environment Limited

Committed to Carbon Reduction and Monitoring

The Visual Environment Ltd Security & Privacy Policy

1.1.1. DATA PROTECTION

- 1.2. Each Party agrees that, in the performance of its respective obligations under this Policy, it shall comply with its respective obligations under the Data Protection Act 1998 as applicable to The Customer as a "data controller" and to the The Visual Environment Ltd as a "data processor" as those terms are defined in such Act and other applicable regulations regarding privacy and information protection. Where used in this Section, the expressions "process" and "personal data" shall bear their respective meanings given in the Data Protection Act 1998.
- 1.3. The Visual Environment Ltd shall not process any personal data provided or made available to The Visual Environment Ltd by The Customer in connection with this Agreement except in accordance with the instructions of The Customer and not for any purpose other than that which is strictly necessary for the performance of its obligations under this Agreement. Without prejudice to the foregoing, The Visual Environment Ltd shall not damage, alter, disclose, lose or destroy any personal data unless instructed to do so in writing by The Customer.
- 1.4. The Visual Environment Ltd shall treat personal data as strictly confidential. The Visual Environment Ltd shall use reasonable endeavours to ensure that only those of its employees, agents and contractors expressly authorised to have access to personal data for the purpose of performing The Visual Environment Ltd's obligations under this Policy shall have access to personal data. The Visual Environment Ltd shall ensure that each employee, agent or contractor may only access personal data for the purpose of performing The Visual Environment Ltd's obligations under this Policy and undertakes to abide by the obligations of The Visual Environment Ltd regarding personal data contained in this Policy.
- 1.5. The Visual Environment Ltd shall not transfer any personal data outside of the European Economic Area without the prior written consent of The Customer and subject to The Visual Environment Ltd entering into such additional agreements as The Customer may reasonably require.
- 1.6. The Visual Environment Ltd shall (and shall ensure that its contractors shall) bring into effect and maintain all reasonable technical and organisational measures to maintain security, prevent unauthorised or unlawful access to or processing of personal data and accidental loss or destruction of, or damage to, personal data. The Visual Environment Ltd shall give The Customer written notice as soon as The Visual Environment Ltd becomes aware of any breach of its data protection obligations under this Agreement or of any enforcement proceeding against it under the Data Protection Act 1998 or other applicable regulations regarding privacy and information protection.
- 1.7. If the subject of any personal data makes a written request to The Visual Environment Ltd for access to any relevant personal data held or processed under this Agreement, The Visual Environment Ltd shall immediately notify The Customer. On receipt of such a request or notice of a request made to The Customer and subject to any other instructions by The Customer, The Visual Environment Ltd shall provide details of the personal data held by it in relation to that person within fifteen (15) days after its receipt of the request or notice of the request for that personal data.
- 1.8. For clarity, it is the intention of the The Visual Environment Ltd not to hold any customer and or account information and or personal data of The Customer.

The Visual Environment Limited
Committed to Carbon Reduction and Monitoring

2. INFORMATION SECURITY AND PRIVACY

2.1. Information Security Program

2.1.1. The Visual Environment Ltd's Information Security Program shall include all Security Requirements as listed below. At The Customer's request and at no cost to The Customer, The Visual Environment Ltd shall make commercially reasonable modifications to its Information Security Program or to the procedures and practices in order to conform to Customer Security Requirements, as they may exist from time to time. The Visual Environment Ltd acknowledges that upon request in order to be allowed continued access to Program Information, it will make modifications to its Information Security Program to add additional measures necessary to retain Information Security standards.

The Visual Environment Limited

Committed to Carbon Reduction and Monitoring

2.2. Privacy Policy

The Visual Environment Ltd's processing of your personal data is governed by the Data Protection Act 1998.

If you have any questions regarding our privacy statement, please contact:

Email : video-miles@thevisualenvironment.com

The Visual Environment Ltd is registered with the Information Commissioner for the United Kingdom.

How do we collect information?

When you contact The Visual Environment Ltd and register to our services, send our Video Analysis form you provide us with optional personal information. Videoconferencing Call Data is automatically sent to the Video-Miles server once a contract is in place. This information is sent via the Video-Miles Fetchit over a SSL connection.

What information do we collect?

Personal information

When you supply information on our Video Analysis form optional information may be included such as your name or email address, we are legally obliged by the Data Protection Act 1998 to ensure that we only use this information for the purpose for which it was requested, and to ensure that it is kept securely.

Videoconferencing Call Data

An example of the information collected is shown below.

System Name	Start Time	Duration	Remote System Name	Call Number
HD System	26/08/2008 16:30	4386	The Visual Environment Calum	84.92.39.118

Call Direction	Number of Attendees	Disconnect Reason	Cause Code
Out	1	The call has ended.	16

The Visual Environment Limited

Committed to Carbon Reduction and Monitoring

What does providing your personal information mean?

When you provide us with personal data, such as your name or email address, you consent to the collection and use of this information for a specified purpose within the Video-Miles® service.

Will we disclose the information we have collected to outside parties?

We may need to disclose your information if required to do so by law.

Do we use cookies?

Yes. Cookies are pieces of information that are sent to your computer by The Visual Environment Ltd when you log onto our website. They are stored on your computer's hard drive, allowing us to recognise you as a user when you next visit.

If you do not want cookies to be stored on your PC it is possible to disable this function without affecting your navigation around the site.

Can you gain access to your personal information?

You may request a copy of the personal information relating to you which is kept on file by The Visual Environment Ltd (for which we charge a fee) by contacting the Data Protection Officer.

Video-Miles@thevisualenvironment.com

Updating my information

If any of your personal information changes or you find that our records are out of date, please email including an updated Video Analysis form highlighting the changes requested. This may incur a fee for changes to System detail.

Video-Miles@thevisualenvironment.com,

System data

When you register with us, you are stating that any information you provide to us about yourself your Videoconferencing systems and subsequent Infrastructure products upon registration or at any time is true.

Confidentiality

We cannot be held responsible for the privacy of data collected by websites not owned or managed by The Visual Environment Ltd.

Notification of change of privacy policy

We reserve the right to amend this privacy statement periodically in order to keep up to date with the changes in our security procedures.

The Visual Environment Limited

Committed to Carbon Reduction and Monitoring

3. SECURITY REQUIREMENTS

3.1. Protection

- 3.1.1. The Visual Environment Ltd shall provide this documented security plan for providing services to The Customer and for hosting or handling Videoconferencing system Information. This plan, at a minimum, shall prescribe the architecture of The Visual Environment Ltd's system, Program Information placement within the system, the security controls in place (e.g. firewalls, web page security, intrusion detection, incident response process, etc.) This plan also describes physical security measures in place to protect Program Information received or processed by The Visual Environment Ltd, including those that will protect Program Information that has been printed or otherwise displayed in forms perceptible with or without the aid of equipment. This plan must be approved in writing by The Customer security Representatives, in The Customer's reasonable discretion, before The Customer will accept The Visual Environment Ltd's services, disclose Program Information to The Visual Environment Ltd or locate Program Information on The Visual Environment Ltd's systems.
- 3.1.2. The Visual Environment Ltd shall install and use a reasonable change control process to ensure that access to its systems and to Program Information is controlled and recorded. The Visual Environment Ltd shall notify The Customer of any planned system configuration changes or other changes affecting the security plan applicable to Program Information, setting forth how such change will impact the security and protection of Program Information. No such change, which could reasonably be expected by The Customer to have a material adverse impact on the security and protection of Program Information, may be implemented without the prior written consent of The Customer security Representative. The Customer may approve these types of changes prior to their becoming effective, such approval not to be unreasonably withheld or delayed.
- 3.1.3. The Visual Environment Ltd shall cooperate with The Customer by conducting security vulnerability (penetration) testing on The Visual Environment Ltd's system, which may include unannounced security penetration tests by electronic methods.
- 3.1.4. Subject to the terms of this Policy and the Schedules attached hereto, The Visual Environment Ltd will take commercial best measures to prevent the unintended or malicious loss, destruction or alteration of The Customer's files, Program Information, software and other property received and held by The Visual Environment Ltd. The Visual Environment Ltd shall maintain back-up files (including off-site back-up copies) thereof and of resultant output to facilitate their reconstruction in the case of such loss, destruction or alteration, in order to insure uninterrupted Services in accordance with the terms of this Policy and its Schedules.

3.2. Detection

- 3.2.1. The Visual Environment Ltd shall monitor its system and its procedures for security breaches, violations and suspicious (questionable) activity. This includes suspicious external activity (including, without limitation, unauthorized probes, scans or break-in attempts) and suspicious internal activity (including, without limitation, unauthorized system administrator access, unauthorized changes to its system or network, system or network misuse or Program Information theft or mishandling). The Visual Environment Ltd shall notify The

The Visual Environment Limited

Committed to Carbon Reduction and Monitoring

Customer promptly (but no later than 24 hours thereafter) of any security breaches or suspicious activities, including without limitation unauthorized access attempts and service attacks, e.g., denial of service attacks.

3.2.2. The Visual Environment Ltd shall allow The Customer to inspect the physical system equipment, operational environment and Program Information handling procedures used by it or any of its Subcontractors providing 48 hours notice of any such inspection is given by The Customer.

3.2.3. The Visual Environment Ltd shall maintain for a mutually agreed-upon length of time, all system records and logs.

3.3. Response

3.3.1. The Visual Environment Ltd shall notify The Customer's Relationship Manager immediately in the event of a breach of security or the detection of suspicious activity.

3.3.2. The Visual Environment Ltd shall cooperate fully with all The Customer's security investigation activities and communication via The Customer's Relationship Manager or through The Customer's security escalation channel, for any escalation and the control of significant security incidents.

3.3.3. The Visual Environment Ltd shall monitor industry-standard information channels (bugtraq, CERT, OEMs, etc.) for newly identified system vulnerabilities regarding the technologies and services provided to The Customer and fix or patch any identified security problem in an adequate and timely manner. Unless otherwise expressly agreed in writing, "timely" shall mean that The Visual Environment Ltd shall introduce such fix or patch as soon as commercially reasonable after The Visual Environment Ltd becomes aware of the security problem. This obligation extends to all devices that comprise The Visual Environment Ltd's system, e.g. application software, databases, servers, firewalls, routers and switches, hubs, etc., and to all of The Visual Environment Ltd's other Program Information handling practices.

3.4. Information Destruction Requirements

3.4.1. Overall Requirements

3.4.1.1.1. The Visual Environment Ltd shall destroy all Confidential Information after it is no longer needed. The Visual Environment Ltd has developed information destruction processes that meet standards and baselines and that will be used in all cases when Confidential Information is no longer needed. These information destruction requirements are to be applied to paper, microfiche, disks, disk drives, tape and other destroyable electronic or digital media containing Confidential Information.

3.4.2. Paper and Other Shreddable Media

3.4.2.1.1. Paper and other shreddable media includes paper, microfiche, microfilm, CDs and any other media that can be shredded. This media is shredded using cross-cut shredding machines when the The Visual Environment Ltd is finished with the Confidential Information contained thereon and it is no longer needed. This

The Visual Environment Limited

Committed to Carbon Reduction and Monitoring

media may be shredded immediately or temporarily stored in a highly secured, locked container. The media may be shredded at a location other than the The Visual Environment Ltd's facilities; however it will be transferred in a highly secured locked container. Confidential Information in this media will be completely destroyed by shredding such that the results are not readable or useable for any purpose.

3.4.3. Electronic Media

3.4.3.1.1. Electronic media includes, but is not limited to, disk drives, diskettes, tapes, USB and other media that is used for electronic recording and storage. This media is to be wiped or degaussed using approved wipe or degaussing tools. Wiping uses a program that repeatedly writes data to the media and thereby destroys the original content. Degaussing produces an electronic field that electronically eliminates the original data and clears the media. These techniques must meet The Customer's standards and baselines. The resulting media must be free from any machine or computer content readable for any purpose.

Video-Miles® Security Information

Fetchit sends data one way only out to the video-miles server through port 80 over a SSL encrypted connection.

There is no remote access to the Fetchit.

The Fetchit is Proxy aware

The Fetchit authenticates to the video-miles server.

Passwords must be 8 chars. or more, contain only alphanumeric chars, at least 1 letter and 1 number and is case sensitive.

Passwords can be changed as and when the customer chooses by logging into the video-miles under my details.

login & change password pages are supplied over a SSL. So any password is sent encrypted.

Video-miles is protected by a Cisco ASA firewall (see attached diag)

There is no direct connection to the database on Video-miles

The visual environment Ltd is a registered company to ICO (Information Commissioners Office) as a Data controller under the Data Protection Act. www.ico.gov.uk.

Physical Security of Video-Miles server(s)

From the car park you come to the entrance, and entry can only be done via a key fob - which only our engineers and data centre staff have. So, any customer must be accompanied by an engineer. The helpdesk at reception requires the customer to sign in - having arranged their visit 24 hours earlier. Engineers have to sign in and out as well. From here they must go to the main control room where data centre staff will give the engineer a new key fob - which he cannot take out of the data centre. With this key fob he can go through the doors to where the servers are kept. There are two more sets of doors, requiring key fob access, between here and the servers. Once in the server area, each server is kept in a rack in cages - each cage requires key access.

There are approximately 6 or 7 barriers to get through before getting to the server(s) - even for our engineers.

Within the facility the temperature is controlled to the optimum level and relative humidity maintained at 45%.

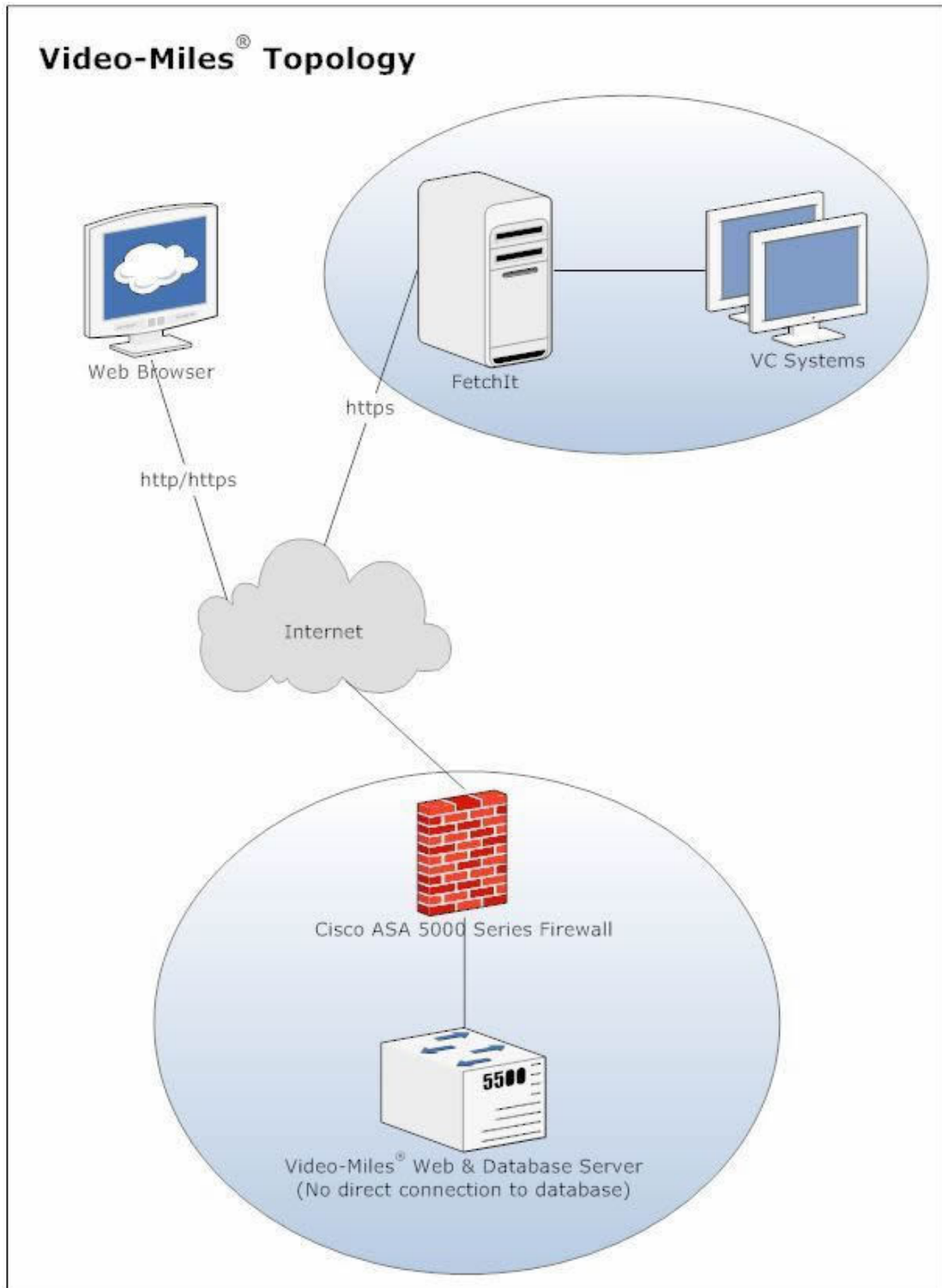
Secure site access and internal CCTV monitoring.


The technical team are available 24/7/365

A sophisticated VESDA fire detection system is in operation and is coupled with CO2 and Halon gas fire suppression systems. This equipment is designed to ensure that any potential fire hazard is detected at a very early stage. In the unlikely event of a fire breaking out the suppression systems will extinguish the fire without damage to valuable equipment.

As well as this the whole data centre is CCTV monitored - with a dedicated team of security personnel monitoring the CCTV 24/7.

The Visual Environment Limited
Committed to Carbon Reduction and Monitoring




Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

DATA PROTECTION ACT 1998
Register Entry Report

Registration Number :

Registered :

Expiry Date:

Data Controller:

Address:

Company's House Registration Number:

Printed 20 02 2008

Page 1 of 4

789