Information Security Policy

Last review V17.0 October 2018

This policy describes Cobalt Sky's approach to handling client data, to ensure that it is kept secure and remains confidential.

See also our Computer Resource Policy on the use of Cobalt Sky's computer systems.

Infrastructure

Cobalt Sky uses a set of internal and external managed secure servers, with appropriate software and patches to minimize vulnerability to unauthorized access.

Internal Servers are kept in a locked room at Cobalt Sky's office, and all server console screens use password protected screensavers. Only authorized people can access the server room and know the screensaver and administrator passwords.

All servers use RAID5 disk arrays; in the event of a disk failure the server will continue to run and the disk can be replaced without downtime, ensuring continuity of service.

All servers are backed up overnight to DLT tapes using NetVault backup software. All backups are encrypted. Backup tapes are stored securely off site. Clients can request that their data is never backed up to tape, in which case we will arrange for it to be backed up to a separate server every night or to a secure online storage provider. Clients may also request their data is excluded from all forms of back up though we must be sure that the client can recreate it in the event of failure of our systems.

Our web servers are managed at IOmart data centres. The following features are applicable to these:

Key features:

- Only UK based servers
- 24 hour Manned Security, CCTV & Intruder Alarms
- 24 hour on site Network Operations Centre (NOC)
- 4 x 1MW Generators
- 0.75 kW/m² power density
- N+1 Air Conditioning Systems
- Dual zone fire detection & INERGEN suppression system
- Up to 63A MCCB's within PDUs
- Dark Fibre Capability & Diverse Fibre Entry
- Carrier Neutral
- 6 x 500 kVA UPS (N+1)
- Controlled Environment - room temperature
- 0.75kW/m² cooling density

- 12kN/m² raised floor system - 600mm void
- Mirrored Switchgear

Maximum Security

- 24 x 7 x 365 Manned Security & Monitoring
- Smart Card access policies
- Internal and External CCTV systems
- Security breach alarms

Power

- Dual independent power feeds, backed up by dual battery string Uninterrupted Power Supplies (UPS) systems (deployed as standard)
- 2 Megawatt diesel generators - protect services from any single power failure

Technical Support & Services

- On site technical engineers 24 x 7
- All technicians are employed direct by iomart
- On site Network Operations Centre (NOC)

Stable Environmental Conditions

- 24 x 7 environmental monitoring systems
- Constant evaluation and testing of all systems
- N+1 redundant Heating Ventilation Air Conditioning (HVAC) system
- Fully redundant air handling units provide constant fresh airflow
- Raychem Fluid Detection
- FM200 fire suppression equipment

Interconnectivity

- Diverse fibre routing via multiple carriers
- Truncated internal cable network
- ODF/DDF (Optical Distribution Frame/Digital Distribution Frame) bandwidth
- Cross Connection to a number of Tier 1 carriers
- Internal inventory systems track all cables, circuits and cross-connects
- Scalable architecture including multiple redundant core switches and routers
- Running Windows and SQL

ISO27001 is applicable to all Web collection servers at IOMART.

We have conducted an independent penetration test of our servers and secured all vulnerabilities.

We run Snort Intrusion Detection Services to monitor attempts to break into our network from outside. The Systems Manager is notified by e-mail of all suspicious activity and reviews it immediately.

Staff can connect from home to the office servers via secure VPN and Remote Desktop Connection; staff only use PCs owned by Cobalt Sky.

The company uses Sophos Endpoint Security anti-virus protection which checks automatically for updates at least daily, and ensures that AV signatures are up to date.

There is a server installation procedure that is followed when a new server is installed. There is a server maintenance procedure that is followed for monitoring and installing server updates.

Infrastructure backup

All servers are connected to an uninterruptible power supply (UPS) which is designed to provide power to all servers for up to 8 hours in the event of a power failure. If we anticipate a longer power failure this gives us sufficient time to get a generator on site to provide continuous power until supply is re-established.

In the event of a major failure of the infrastructure, making the servers inaccessible, we can utilize off-site disaster recover servers and be running a service within 12-24 hours.

Client data handling – receiving data

Client data is normally received by e-mail and copied directly to our servers. Once the data has been checked to ensure it can be read, the e-mail is deleted. In cases where the e-mail contains additional relevant information just the attachment is deleted.

Larger files may be provided by secure FTP or Dropbox and are deleted from the server once successfully copied into our production system.

If the data is provided on physical optical media such as CD or DVD the disk is destroyed after the data has been copied successfully to the server.

If the data is provided on a memory stick, the file is deleted from the memory stick once it has been copied successfully.

If the client is sending us personal identifiable information (PII) then it is encrypted and the password conveyed to us by phone or in a separate e-mail. We keep a record of all files containing PII in a separate log file, and such files are deleted within 30 days of project completion.

Staff must not under any circumstances store any information on their PCs. All information is stored on company servers in the appropriate client and project folders. Personal or confidential information may be stored in the user’s home folder on the server.

Certain staff use laptops and may therefore have client information retained on them such as e-mail files. All laptops are encrypted and can only be started with a password. If a laptop is stolen or mislaid the information will be inaccessible to third parties.

Client data handling – storage

Client data is stored until the person responsible for the project deems it ready to be archived. Archiving takes place at least quarterly and projects are copied to DVD and deleted from the servers. Archive DVDs are stored securely on site in the locked server room. A second copy is stored securely off-site.

Mobile devices can be plugged into the usb connection on a PC for the purposes of charging but file access is blocked through policy. Any mobile device which is permitted access to mail is named and can be remotely wiped in case of loss.

Client data handling – sending data

If we are sending data to a client we will normally send this by e-mail. If the information is confidential or personal we will encrypt it using a method acceptable to the client. The encryption password is given by phone or in a separate e-mail.

If the data is too large for e-mail we will normally send it via secure FTP or Dropbox.

Document handling

This procedure is for non personal related information, it is for documents that are either commercially sensitive or client specific and that should be kept confidential and secure.

Client documents are normally received by e-mail and copied directly to our servers. Once the documents have been checked to ensure they can be read and are complete, the e-mail can be deleted. In cases where the e-mail contains additional relevant information then this should also be copied to the project folder both parts can then be deleted.

As with data any larger files may be provided by secure FTP or Dropbox and are deleted from the server once successfully copied into our production system.

If any files are provided on physical media such as CD or DVD the documents will be copied off that media and then the disk is destroyed.

All documents are stored on company servers in the appropriate client and project folders, they are clearly labeled and versions can exist should the need arise but will be clearly identifiable.

Certain staff use laptops and may therefore have client information retained on them such as e-mail files. All laptops are encrypted and can only be started with a password. If a laptop is stolen or mislaid the information will be inaccessible to third parties.

Client documents are stored until the person responsible for the project deems it ready to be archived. Archiving takes place at least quarterly and projects are copied to DVD and deleted from the servers. Archive DVDs are stored securely on site in the locked server room. A second copy is stored securely off-site.

If we are sending documents to a client we will normally send this by e-mail. The client may request that any information is treated as confidential then, if so then we will encrypt it using a method acceptable to the client. The encryption password is given by phone or in a separate e-mail.

If the documents are too large for e-mail we will normally send it via seucre FTP or Dropbox.

Desktop security

Valid logins and passwords are required to access the Cobalt Sky infrastructure. Passwords are changed every 90 days. Strong passwords of 14 characters using a combination of upper and lower case, numbers and punctuation are required. A password must be different to the previous 24 passwords.

When people leave their desks a screensaver automatically locks the screen after 10 minutes, and the user's password is required to unlock the screen.

If a member of staff leaves, all passwords may be forced for immediate change at the discretion of the Systems Manager and Managing Director depending on their assessment of the person leaving.

The VPN password is also changed and staff must request this by phone from the Systems Manager when next accessing the VPN. The server accounts of the departing employee are disabled.

Staff are not permitted to use portable storage devices to copy or move files to or from Cobalt Sky's systems without explicit permission from the Managing Director. USB usage is monitored by Sophos Endpoint Protection and reviewed daily.

Staff are not permitted to install any programs on their PCs without the permission of the Systems Manager.

Internet access is routed through a proxy server. Executables, audio and video files cannot be downloaded from the Internet.

Physical security

An electronic pass is required to access the building lobby, the circulation space and the Cobalt Sky office. Each member of staff has a unique electronic pass, as well as a unique remote fob for activating/deactivating the alarm system. All uses of the pass and alarm activation/deactivation are logged by the building security company.

When an employee leaves, their card and alarm fob are returned to the office manager. The building security company removes access permission for this person and the card and fob are returned to them. New employees are given fresh cards on joining and an alarm fob once they have worked satisfactorily with us for at least three months, and need to access the office when no one else is there.

Review of computer accounts

The Systems Manager and Managing Director review the list of accounts on the servers every three months to ensure that only current staff have access to the systems.

Staff disciplinary procedures

Any breach of the above procedures by a staff member would instigate a staff disciplinary action.

The incident would be investigated under the disciplinary rules and an appropriate action would be taken should the staff member have breached the security rules. This disciplinary action could range from re-training or written warnings through to instant dismissal or further legal actions.

Data protection act

In addition to the above procedures we are registered under the data protection act – Registration Number Z1598099