Data Security Policy

This document covers the following aspects:

- Physical Security
- Firewall and Patch Management
- Incoming Data Files
- Data Retention & Deletion
- Backups
- Personnel
- Approach to Risk and IS Asset Register

Physical Security

Ciconi operates out of one central building located on Warboys Airfield Industrial site. There is an alarm system in place and each night the premises are locked and the alarm is set when there is no-one on site.

The alarm monitoring company is Custodian, which will contact an appointed key holder if one sensor is triggered.

If more than one sensor is activated, then Custodian contact the police as well as the appointed key holder.

During working hours, site access is restricted, as all personnel are issued with a key fob in order to enter and exit the building. The roller shutter doors used in Production are only opened when there is a delivery and are not used as an entry point.

The side door and roller shutter doors in Production are locked when the Production area is unattended.

Any scheduled visitor at Ciconi has to call in on the door intercom system before access is granted. They are then let into the reception area and met by a Ciconi employee, who is responsible for them during their visit.

Any unscheduled visitor is asked to wait outside of the building and not granted access until they have been met at the door to establish the purpose of their visit.

Firewall, Patch Management and Virus Checks

Ciconi uses WatchGuard Firewall to protect its servers and keeps all relevant ports shut in order to avoid unwanted items coming onto the servers. Ports 80 (http) and 443 (https) are open and WatchGuard is used to ensure that these are monitored and protected.

The IT Manager is responsible for the maintenance of WatchGuard and ensures that any updates to the Firewall are carried out.

Port 25 is open for Ciconi's Exchange Server to allow incoming and outgoing emails. This is monitored and scanned by Mimecast and maintained by the IT Manager. Mimecast scans all the

emails coming in and going out to maintain a high level of security and avoid unwanted viruses coming in.

The IT Manager completes the patch management on a monthly basis to ensure that all updates are carried out in a timely manner. In addition to this, every quarter, virus checks are also completed to ensure that nothing has slipped through.

Incoming & Outgoing Data

All data that comes in and goes out of Ciconi from clients, suppliers and any other external organisations have to be sent or received via one of the following:

- Liquid Files Server
- Secure File Transfer Portal (SFTP), either the client's portal or Ciconi's portal

Sending and receiving data through Liquid Files means that the file is automatically encrypted to 256-bit and does not require this to be manually done by the sender. Any files that are being sent from Ciconi are done so using Liquid Files.

If the organisation sending data has an SFTP set up then they can allow access for Ciconi staff members to access this portal and send and receive files. Files being sent using SFTP do not need to be encrypted prior to sending as the portal is a secure transfer method.

There is also the option for an organisation to send data using Ciconi's SFTP. This is only accessible on Ciconi's premises as it is linked to Ciconi's IP address and is not cloud based.

Data Retention & Deletion

All data received by Ciconi from clients are saved in secure folders on the network. Only approved members of staff have access to this data.

In addition to this, every year, each member of the Ciconi team re-sign the company's confidentiality agreement, which ensures that all data that they come across or work with is treated as confidential to Ciconi and that all possible means to safeguard the data are undertaken.

Ciconi's normal procedure is to keep client data on the systems until the relevant job has been fully completed, invoiced and paid. Once payment has been received for a job, the data is automatically deleted from the system.

This is maintained and managed by the IT Manager who also completes a manual check to ensure that no data is kept after this point.

Some of Ciconi's clients specify that they would like to have data re-used for a subsequent job or ongoing campaign. Therefore, Ciconi does offer the client an option to exclude their data from the automatic deletion to allow the data to be re-used.

In these cases, the secure folders are checked monthly by the IT Manager, who informs Customer Services what data is on the system. The client can then decide if the data needs to be kept or deleted.

Backup Policy

There are daily and monthly backups completed at Ciconi. Daily backup tapes are made each evening and overwritten after seven days.

Monthly backup tapes are kept for two years and then overwritten. During this time, the tapes (both the daily and monthly), are stored in a fireproof safe (up to 120 minutes fire resistant) on site, which only the IT Manager, IT Executive and Company Designer can open. For additional security, the tapes are also encrypted and the safe is located in the server room, which has a key pad to enter and only approved staff members have access.

Client data is excluded from the monthly backup routine and only ever included on the daily backup.

Personnel

In addition to the confidentiality forms that are signed by all staff members, other precautions are taken to ensure that all data handled at Ciconi is safeguarded.

To get on the Ciconi network, each employee has their own log on details and password. There is no tolerance for the re-use of passwords and the passwords have to comply with the following:

- The password has to be a minimum of 8 characters
- The password has to have a minimum of 2 numbers
- The password has to have a minimum of 4 letters

Under no circumstances are passwords shared.

In addition to this, all employees ensure that their PCs are locked when left unattended and a clear desk policy is active and in place to have all confidential information removed from sight.

Approach to Risk

Ciconi is certified for ISO27001 and as part of this there is a procedure in place for risk assessment of threats and vulnerabilities applicable to protected information. Zero risk does not exist, however Ciconi completes a risk assessment to reduce risk where possible. Residual risk is reviewed and accepted by the Senior Management team at Ciconi and any actions arising from this are actioned to reduce the risk. This is reviewed at least annually and actioned by the IT Manager as well as the Senior Management Team.

If a security breach was found, a log of this would be recorded and the breach would be investigated and resolved as quickly as possible. An additional risk assessment would be conducted to search for any gaps and prevent re-occurrence.