Connevans Limited Data Management & Information Technology Security Policy

Connevans Limited depends on Information and Communications Technology (ICT) systems to operate. Security of these systems and the data they hold, and of the hardware and networks on which they operate is necessary both to honour our obligations to providers of data (customers, suppliers, staff etc) as registered under the Data Protection Act, and to protect the company's systems, devices and data from accidental or deliberate damage, loss or corruption. This policy statement is intended to effect implementation of the overall information security policy in respect of data held in ICT systems and on any electronic device. All staff have a responsibility to comply with the Connevans policy on confidentiality of data and data security.

The key points of our strategy are as follows:

- Data is owned by Connevans Limited and is the responsibility of the Management Team, who are accountable for the security of that data and determine the standards of confidentiality that are to apply.
- All staff and customer personal data is maintained only for the purpose defined within the notification under the Data Protection Act.
- Access to our data stores is limited to those needing such access to do their job and the system design facilitates such access. Each member of staff with such access is personally responsible for maintaining the confidentiality of the data to which he/she has access.
- Data whether in electronic or physical form is subject to physical security control appropriate to its nature. Physical access is determined on the same basis as data access unless there are over-riding security reasons for doing otherwise.
- General facilities such as e-mail and conferencing are provided solely for business purposes and the data generated by these is treated as belonging to the company.
- Data may be held on central servers, the company portal, personal workstations, portable devices such as laptop computers and smartphones, and other removable media such as readable CD's/DVD's and USB flash drives. Data held in central locations are the responsibility of the IT Supervisor. They will be responsible on behalf of Data Owners for the security of data deposited on these servers. Security of data held on personal workstations, portable storage devices or on associated removable magnetic media (including video recorders) is the responsibility of the individual member of staff who operates the equipment.
- Responsibility for the security of the Connevans Limited network (including software, hardware and general services) rests with the IT Supervisor on behalf of the Managing Director. This responsibility is limited to the security of data in transit and ends when the data is delivered to its destination.

- System specifications define the requirements for back up copies of programmes and data appropriate to the requirements of the system as determined by the IT Supervisor, institutional and legal requirements.

- Contingency disaster plans are required for core systems and are administered and authorised by the Business Recovery Team (See Business Continuity Management Plan). The BRT is also responsible for IT Security Incident response and escalation, in accordance with the Business Continuity Management Plan.

- All staff have a personal responsibility to safeguard the integrity and confidentiality of the company's systems, data and physical facilities. Line management is responsible for the application of the data security policy for matters under their control. They must ensure that all staff are aware and comply with the policy. Breaches in security could lead to disciplinary action.

Cardholder data

Where we are in possession of customer cardholder data (card number, cardholder name, expiration date and/or service code), this is only to be retained for as long as is necessary to allow us to complete the appropriate business processes.

Access to Cardholder data is restricted to those who have a genuine business case and it is not to be stored in any electronic format. On no occasion, is cardholder data to be sent electronically, by any messaging method, to a colleague within Connevans Limited or to the customer.

All staff who may come in contact with cardholder data or the payment device during the course of their work undergo compulsory training on data security, compliance with this policy, awareness of suspicious behaviour and detecting whether a device has been tampered with. They are required to report any concerns to the IT Supervisor.

Appendix A of this policy is a list of all devices that capture payment card data. This list is the responsibility of the IT Supervisor and must be fully updated and maintained at all times.

To ensure we meet these commitments we will review our data security policy annually.

General information security

The IT Supervisor controls access to all critical technologies (computers, laptops, tablets, smartphones etc). Authorised staff are issued with a unique username and password, which is not to be shared with colleagues. The IT Supervisor is responsible for maintaining a list of users which is to be kept secured at all times.

All staff and users must comply with the Connevans Limited IT Acceptable Use Policy – see Appendix B.

Access to our systems or data by third party partners is strictly controlled and limited according to what is required and reasonable to allow them to execute their service. all suppliers go through a process of due diligence prior to instruction and ongoing monitoring by their internal point of contact throughout the life of the contract.

Remote access to our systems is only given to people who require this to carry out their job roles. Access is carefully managed and restricted and all approved staff are required to undergo appropriate training.

David Evans
Managing Director
January 2019