Data Security Policy v2

Policy Overview

CCR Data/Mailing Ltd is comprised of management, staff, temporary workers, contractors, investors, shareholders, business partners and will herein be referred to as "CCR".

CCR takes very seriously our Data Security Policy. We have taken great care to ensure the safety of the often confidential information entrusted to us by our clients. We work with partners such as The Royal Mail, BSI, and Experian to achieve the highest levels of security when handling client data.

Our security is based on ISO 27001/2 which is used by the Royal Mail as a pre-requisite to becoming a Royal Mail accredited data bureau. The Royal Mail performs a regular audit to ensure that standards and new working practices are adhered to.

These policies and standards outline the core requirements for all of CCR when handling its clients.

Physical security

In accordance with regulatory and contractual requirements the premises on which CCR conducts its business must be risk assessed and policy managed, this ensures the protection of both the interests of the client and CCR.

- Electronic door entry system on entrance doors.
- Coded entry systems on key internal doors, such as server rooms and opening rooms.
- ADT alarm system
- CCTV in opening room
- 3 Data safes
- 24 hour security guard on gated vehicle entrance

CCR should also have the following information to hand in case of an emergency scenario in which the information may be needed:

- Fire protection policy
- Grounds and office risk assessment
- Evacuation and threat response procedures
- Process for activation of the business continuity plan

IT Hardware

Regulatory and contractual requirements for the premises also demand that our hardware can protect all interested parties.

- Hardware based Firewall (Fortigate).
- Our firewall is managed and maintained by a 3rd party who run regular vulnerability tests.
- All servers housed in racks in a secure coded lock based server room that applies to all the standards set out above.
- Regular audit of IT hardware and software
- Password policy including requirement to change every 28 days
- Spare connections are physically disconnected from the patch panels so "extra" equipment can only be connected on an authorised basis.
- IT policy prevents the connection of other devices such as MP3 players or USB key drives or hard drives for all staff.

CCR Data/Mailing Limited, Unit 4, Minton Distribution Park, London Road, Amesbury, Wiltshire, SP4 7RT
☎ 01980 592999 Tel ☎ 01980 592929 Fax ✉ info@ccr.co.uk www.ccr.co.uk

Data Security Policy v2

Data Handling

When receiving or transmitting data to or from the CCR infrastructure it is vital that the following conditions are met in accordance with regulation policy, NDA and any SLA's put in place to ensure levels of service provision to the client.

- No data is sent from the CCR network without security using either SFTP or encryption using "Utimaco Safeguard Private Crypto" software as a minimum unless a specific request is made by the customer in writing beforehand.
- Data is only shared with Experian as per our standard NDA as the services CCR provide may be Experian services and not entirely CCR Data/Mailing Ltd's own.
- CCR can provide secure FTP or other secure endpoints on demand in order to allow customers to send data to us securely but this is not a requirement needed by all customers.

Data sent from the client to CCR must be used only for the job it is specifically intend unless prior authorization is provided by the client in writing, in order to carry out the job CCR may need to share the client data with carefully selected partners during which it is the responsibility of CCR to ensure that the data is protected from intrusion, attack, theft, or unintended modification.

Backups

Incremental backups are performed daily of all business critical and customer data. Copies of the daily backups are kept in a secure safe off site in case of emergency for business continuity.

The data is removed from our servers and hard drives 3 months after client settlement, this data will then only be available for 12months before being removed completely from our backups

Data submitted via FTP/SFTP will be removed within the shortest time period possible, at a maximum of a couple of weeks; however it will still be available, via the above process.

Client Data Obligations

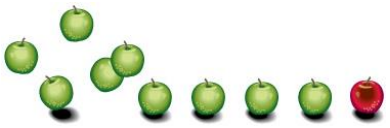
Compliance to regulation and policy or standard process dictates that all personnel must be aware of and understand their obligations regarding client or other sensitive data, NDA's cover many key points but the following must also be adhered to in order to ensure CCR and the client are both protected.

Users are obligated to respect the confidential nature of the business and the relationship of CCR with its client and protect the interest of the client at all times, the user must never knowingly copy data from the CCR infrastructure to any other location unless explicitly requested in writing by the customer.

Data provided by the client must be protected by the user by ensuring that no data is left on an area of the network that is not approved for storage by the board of directors.

Client data must never knowingly be deleted or altered without prior authorization from the client.

Client data or other confidential information must not be left on unattended desks to ensure that the client interests are upheld.



CCR Data/Mailing Limited, Unit 4, Minton Distribution Park, London Road, Amesbury, Wiltshire, SP4 7RT
☎ 01980 592999 Tel ☎ 01980 592929 Fax ✉ info@ccr.co.uk www.ccr.co.uk