



# Icicle Business Information Security Standard for **Direct Mail Data Handling**

## Background

To safeguard our client's customer data, Icicle requires that the production of "data merge" jobs be carried out in secured environment and systems that comply with / observe:

**HKMA Supervisory Policy Manual on Outsourcing**

**The Code of Practice issued by the Privacy Commissioner for Personal Data**

**Icicle's own information security requirements**

As we act as the "data merge" service provider for many financial institutions, including retail banks, credit card companies, investment banks etc., Icicle has comprehensive policies and procedures in place for safeguarding the customer data during transmission, processing, production and delivery. Below is a shortlist for your reference.

- ◆ Information security policy and procedures
- ◆ Hiring policies
- ◆ User account administration policy
- ◆ User entitlement reviews
- ◆ Employee non-disclosure agreement
- ◆ Information security incident report policy
- ◆ Internal audit
- ◆ External audit conducted by third party
- ◆ Physical security policy and procedures
- ◆ Key data centre critical personnel
- ◆ Building access and log files
- ◆ Security requirements on operating systems, applications, network for systems processing of clients' customer information
- ◆ Security log review
- ◆ Network diagram to store or process clients' customer information
- ◆ Systems backup
- ◆ Tape Management system
- ◆ Vulnerability and threat management scan
- ◆ Anti-virus deployment
- ◆ Standard server /workstation configuration guide
- ◆ Change management and problem management
- ◆ Continuity of Business