Data Security Policy

Processing Centers

2017 --- 2018

1 . Introduction

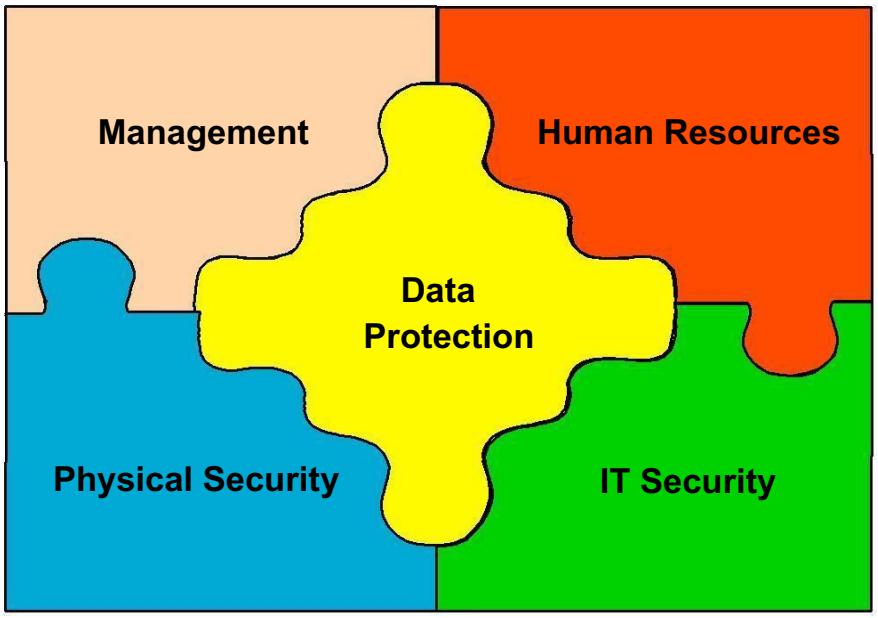
This document covers the policies and procedures that Virtual Data Partners (VDP) adheres to for data security within our data processing centers. Using this model, VDP does a continuous monitoring of risk vis-à-vis the data and the information assets for confidentiality, integrity and availability.

2 . Data Protection Controls

Data protection controls are categorized in the following.

- Management control
- Human Resources control
- Physical Security
- IT security

The details of each layer are described in the following sections.



2.1 Management Controls

A. Security Policy: VDP issues a security policy to keep all the stake holders informed. The policy is:

- Approved
- Regularly Reviewed
- Version controlled

B. Audit

- Periodic review of Information Security within the organization
- Semi-annual external cybersecurity audit on all information systems
- Incident Reporting

2.2 Physical Security

- Security personnel operating.
- No local file storage facilities onsite - environment is completely virtualized via Amazon Web Services and Dropbox with 2-factor authentication in place.
- All the employees involved on projects are given training on security, privacy and confidentiality. We have disabled all the external drives in the systems and the ability to extract information onsite.
- Paper/printed documents are not allowed: Our employees are not allowed to bring in or take out any paper, printout or written documents without permission.
- The offices have smoke alarms and multiple fire extinguishers.
- CCTV Monitoring is carried out onsite and reviewed periodically.
- Offices have security measures to prevent the vandalism or theft of any information stored in our systems.

2.3 IT Security Controls

- Password Policy (Complexity, Length, Age, Lock Out Attempt, Lock Out Period, Generation, Auto Screen Lock-out).
- Access Rights managed at/with active directory.
- Recordable Media and other devices disabled for the desktop users.
- No local admin rights for the desktop users.
- Exceptions may be allowed depending on project requirement.
- Server and back-end systems are completely virtualized and hosted on Amazon Web Services and Dropbox with 2-factor authentication in place.

2.4 HR Information Security Controls

- Orientation.
- Confidentiality agreements.
- Training.
- Security awareness.
- Access privileges change management.
- Periodic review of physical & logical access.
- Password management activity.
- Retrieval of company assets during exit.

2.5 Network Infrastructure

- Antivirus software installed on machines with HIPS (host intrusion prevention) and NAC (network access control).
- Gateway level Anti Spyware and Spam filter for Internet access & mail server.
- URL filtering application for surf control.
- Policy based access to various protocols.
- Physical access controlled by electronic access control.
- Domain level access restrictions along with Group Policy.
- High speed fiber internet connection with backup wireless solutions as redundancy.