

CHÍNH SÁCH SAO LƯU DỮ LIỆU

1. PHẠM VI ÁP DỤNG:

Chính sách này được áp dụng cho tất cả người lao động đang sử dụng các thiết bị vi tính nối với mạng máy tính của Công ty Cổ phần Mạng I.O và Công ty TNHH Một thành viên Truyền thông Tương tác Trực tuyến.


2. MỤC ĐÍCH:

- 2.1 Thiết lập sự phân quyền rõ ràng về truy cập và quản lý thông tin.
- 2.2 Tích lũy tri thức làm tài sản trí tuệ của công ty.
- 2.3 Bảo đảm sự phục hồi và sự tiếp tục hoạt động của các dữ liệu và hệ thống quan trọng.

3. QUI TRÌNH SAO LƯU DỮ LIỆU:

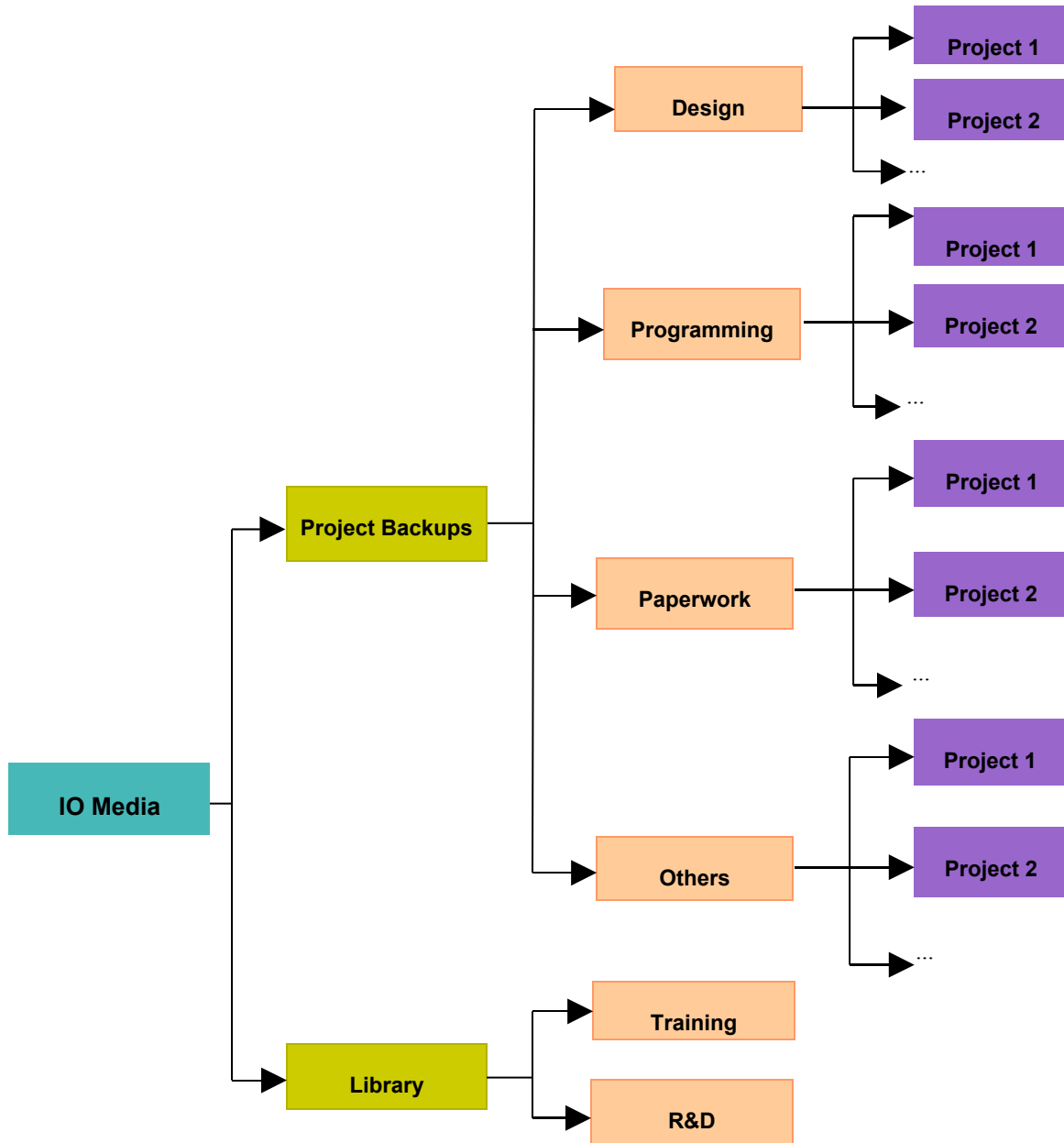
Tất cả việc lưu trữ dữ liệu đều phải tuân thủ chặt chẽ các qui trình sau:

3.1 Nơi thực hiện sao y trong hệ thống mạng máy tính của công ty:

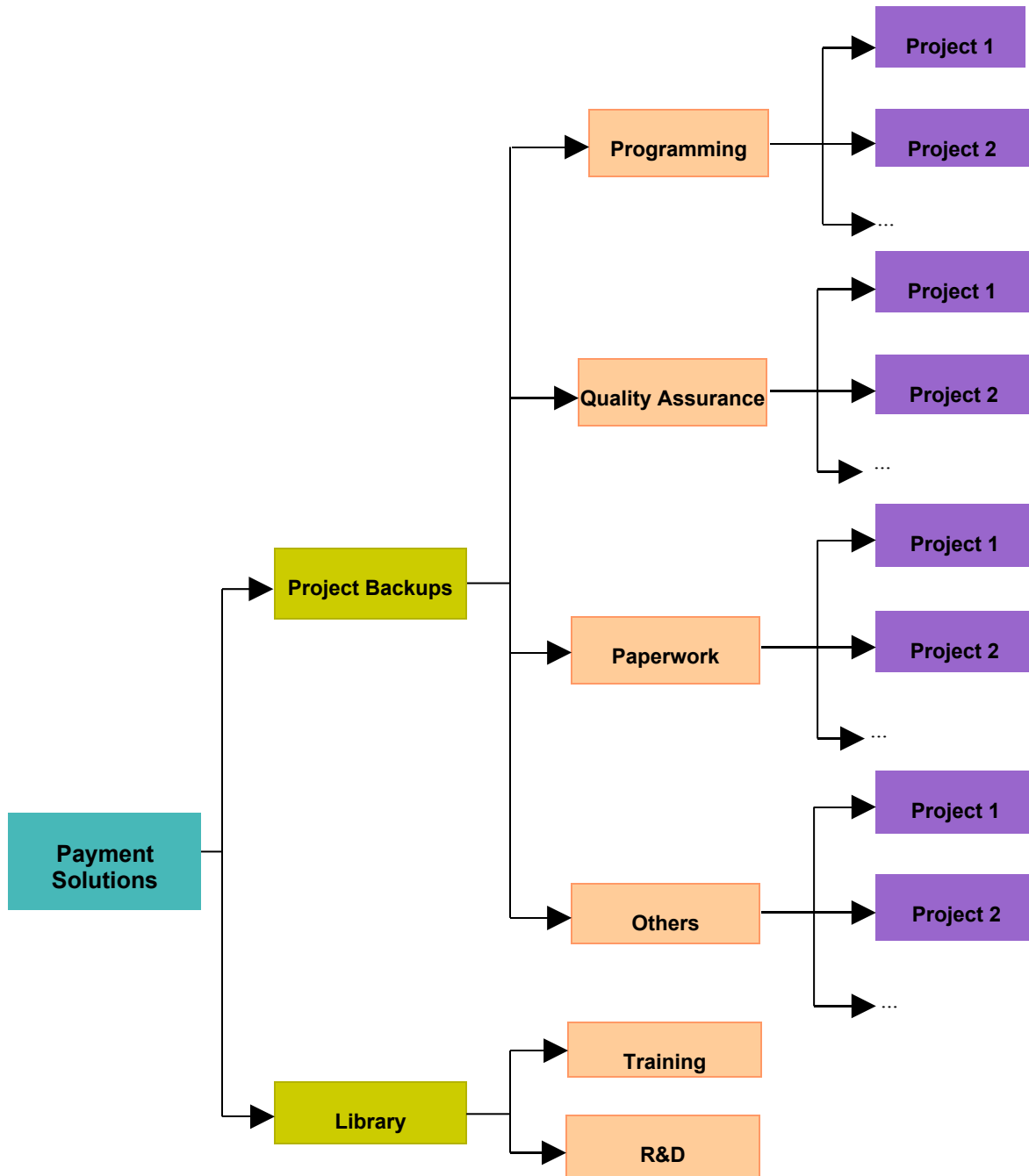
- Đối với các máy tính sử dụng hệ điều hành Window:
 - Nhấn  + E để vào My Computer
 - Trong khung Address: đánh \\filesaver
- Đối với các máy tính sử dụng hệ điều hành Ubuntu:

Đường dẫn: [Places](#) (trên thanh menu của Desktop)/[Network/Windows](#)
[Network/IOSYSTEM/FILESERVER](#)

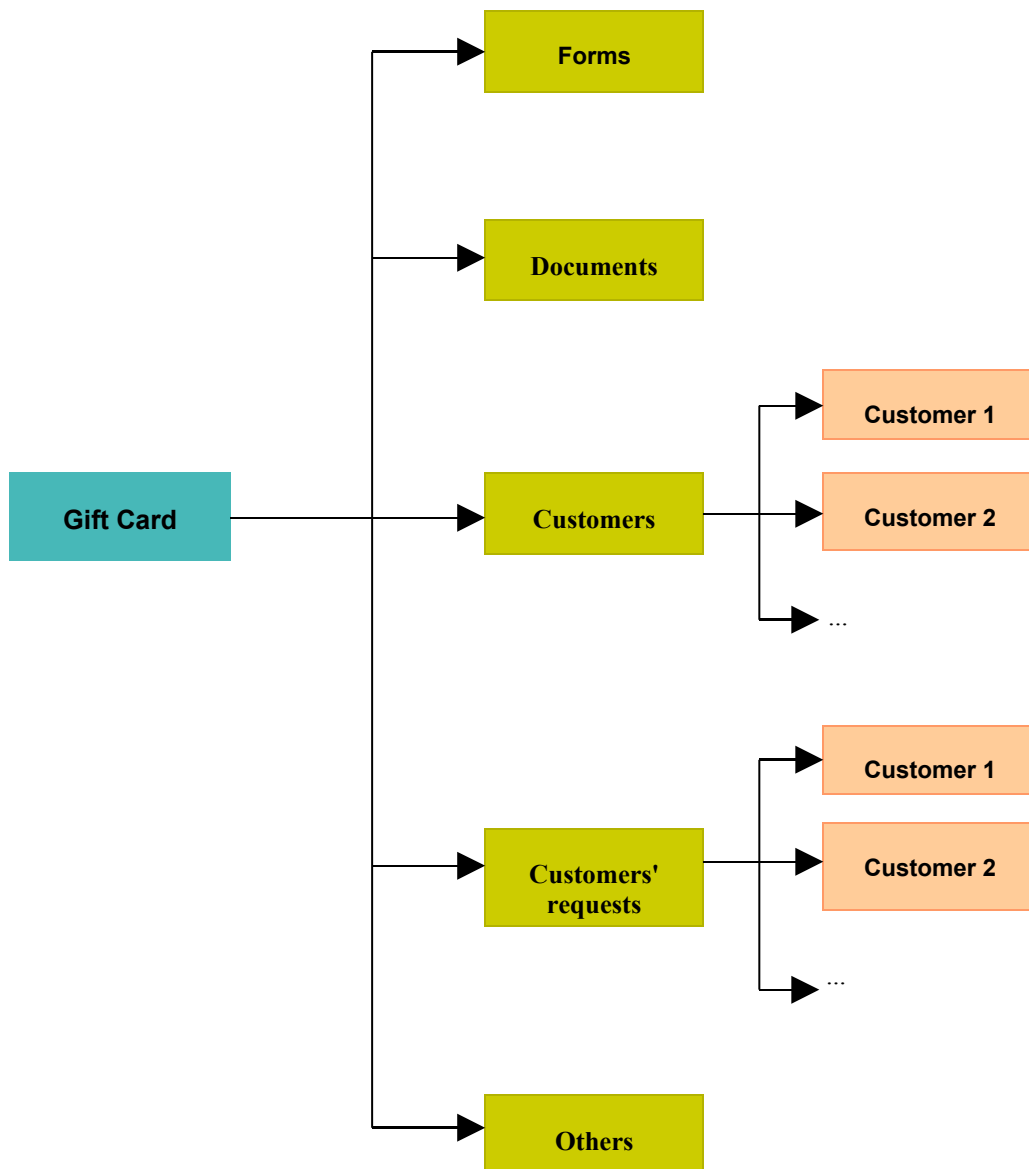
- Trong \\fileserver bao gồm:
- Các thư mục chính và thư mục phụ dành cho IO Media:



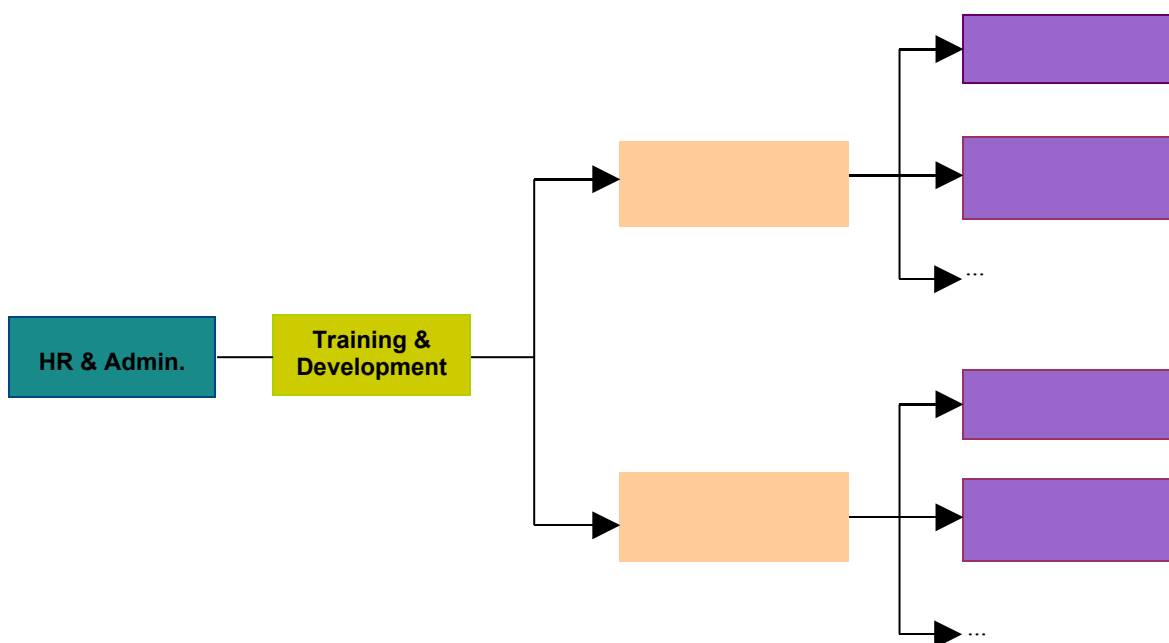
- Các thư mục chính và thư mục phụ dành cho bộ phận Payment Solutions:



- Các thư mục chính và thư mục phụ dành cho bộ phận Gift Card:



- Đối với Phòng HC-NS: Ngoài các dữ liệu được sử dụng để phục vụ cho chức năng Đào tạo và Phát triển, Phòng HC-NS chỉ sao chép và lưu trữ dữ liệu tại 3 nơi: (1) trong máy tính của chính nhân viên; (2) bằng giấy tờ; (3) bằng đĩa CD. Tuyệt đối không được lưu trữ dữ liệu trong server của công ty.



- Đối với Phòng Kế toán: Phòng Kế toán chỉ sao chép và lưu dữ liệu tại 3 nơi: (1) trong máy tính của chính nhân viên; (2) bằng giấy tờ; (3) bằng đĩa CD. Tuyệt đối không được lưu trữ dữ liệu trong server của công ty.

3.2 Qui định đặt tên cho dự án:

Năm bắt đầu dự án . Năm kết thúc dự án . Tên Khách hàng . Tên Dự án

VD1: 2009.2009.SQUARE. SamsungEvent

VD2: 2009.INDEFINITE.IOMEDIA. Xe Dap Doi

3.3 Số bản lưu:

- Đối với bộ phận IO Media, Payment Solutions và dịch vụ Gift Card: Mỗi đơn vị dữ liệu được tạo thành 03 bản và được lưu trữ tại 3 nơi: (1) trên máy tính của chính nhân viên; (2) trên server; (3) trong đĩa CD
- Đối với Phòng HC-NS và Phòng Kế toán: Mỗi đơn vị dữ liệu được tạo thành 03 bản và lưu tại các nơi như đã mô tả tại (3.1)
- Khi một người lao động nghỉ việc, Trưởng Bộ phận có trách nhiệm phối hợp với nhân viên Quản trị Mạng rà soát lại dữ liệu trong máy tính của nhân viên, thực hiện các sao lưu cần thiết tại các nơi qui định và xóa toàn bộ dữ liệu lưu trên máy tính của người lao động đã nghỉ việc.

3.4 Mức độ về tính quan trọng, Quyền truy cập, quyền quản lý và quyền xử lý dữ liệu:

3.4.1 *Mức độ về tính quan trọng*

“Confidential”

- Những dữ liệu “confidential” bao gồm (nhưng không dừng lại ở những loại này)
 - Tất cả dữ liệu về tài chính kế toán
 - Hợp đồng
 - Kế hoạch kinh doanh
 - Các thông tin về việc đàm phán với khách hàng.
- Chỉ có trưởng bộ phận liên quan và Giám đốc Điều hành có thể tiếp xúc dạng dữ liệu này.
- Dữ liệu dạng này sẽ không được lưu giữ trên server mà phải sao chép trực tiếp ra CD/DVD

“Limited”

- Dạng dữ liệu này chỉ được lưu hành hạn chế trong phạm vi trưởng bộ phận một nhóm người trong bộ phận được chỉ định

“Departmentally Limited”

- Dữ liệu ***“Departmentally Limited”*** được phép lưu hành trong một bộ phận. Tất cả nhân viên trong bộ phận đều có thể tiếp xúc dữ liệu này.

“Public”

- Dữ liệu ***“Public”*** được phép lưu hành trong toàn công ty. Tất cả nhân viên đều có thể truy cập đến dữ liệu này.

3.4.2 Quyền truy cập:

- Mỗi người lao động sẽ được cấp một mật mã để truy cập vào các thư mục.
- Giám đốc Điều hành được cấp quyền truy cập vào tất cả các thư mục.
- Giám đốc Nhân sự được cấp quyền truy cập vào tất cả các thư mục thuộc Phòng HC-NS và các thư mục “Thư viện” của các bộ phận khác.
- Trưởng Bộ phận được cấp quyền truy cập vào tất cả các thư mục của bộ phận.
- Quyền truy cập của cấp nhân viên được giới hạn trong các thư mục liên quan trực tiếp đến công việc chuyên môn.
- Khi một người lao động nghỉ việc hoặc khi được Giám đốc Điều hành yêu cầu, nhân viên Quản trị Mạng có trách nhiệm cắt ngay quyền truy cập của người lao động.
- Nhân viên Quản trị Mạng có trách nhiệm lập và lưu trữ danh sách các nhân viên được cấp quyền truy cập.

3.4.3 Quyền quản lý và xử lý dữ liệu:

- Tất cả nhân viên, trưởng bộ phận phải tự đánh giá mức độ quan trọng của dữ liệu.
- Mức độ quan trọng của dữ liệu có thể được thay đổi bởi Trưởng Bộ phận có liên quan hoặc bởi Giám đốc Điều hành nếu thấy cần thiết.
- Nhân viên Quản trị Mạng có trách nhiệm kiểm tra và cập nhật thường xuyên tình hình sao lưu dữ liệu.

- Trưởng Bộ phận có trách nhiệm thực hiện việc sao lưu dữ liệu trên đĩa CD và chuyển về Phòng HC-NS để lưu trữ.
- Tất cả các dữ liệu được lưu trữ trong server đều mang tính chất “chỉ đọc” (read-only) và không thể chỉnh sửa, xóa hoặc di chuyển được.
- Ngoại trừ Nhân viên Quản trị Mạng, tất cả các nhân viên khác không thể xóa bỏ dữ liệu trên server.
- Cứ hai tháng một lần, Trưởng Bộ phận có trách nhiệm phối hợp với Nhân viên Quản trị Mạng để lập danh sách các tập tin dữ liệu không còn có giá trị sử dụng để thực hiện việc hủy bỏ.
- Nhân viên Quản trị Mạng phải thường xuyên kiểm tra khả năng phục hồi dữ liệu từ các bản sao lưu để đảm bảo các bản sao có thể sử dụng được trong các trường hợp khẩn cấp.
- Chức danh duy nhất có thể phê duyệt việc hủy bỏ các dữ liệu là Giám đốc Điều hành.
- Khi gặp phải dữ liệu bị nhiễm virus, người quản trị mạng phải thông báo cho Giám đốc Điều hành và trưởng bộ phận quản lý dữ liệu đó và đề xuất hướng xử lý.

4. THỜI HẠN THỰC HIỆN:

Ngày hiệu lực: 01.08.2009

5. VIỆC XEM XÉT LẠI VÀ CẬP NHẬT:

Chính sách này sẽ được xem xét lại và cập nhật hàng năm hoặc khi xét thấy cần thiết.

TP. HCM, ngày 28 tháng 07 năm 2009

(Đã ký)

NGUYỄN PHÁT VĨNH LỢI

Giám đốc Điều hành