	<b>ISO 9001-2008 PROCEDURE</b>	<b>PROCESS OWNER</b> Information Technology Management		
<b>PROCEDURE TITLE:</b> Infrastructure - Technology	DOCUMENT NUMBER: ISO_6-3b	REVISION LEVEL: Final Draft	REVISION DATE: 04/20/09	Approval: Managing Director

**Purpose/Scope:**

This procedure defines requirements for the management and maintenance of technology information needed to support the work of the Washtenaw County Road Commission.


**Responsibility:**

Information Technology Management, under the supervision of the Managing Director, is responsible for management and maintenance of all records (hard copy and electronic) as well as all hardware and related physical inventory pertaining to Information Technology.

**ISO 9001:2008 Reference:** 6.3 - Infrastructure

**Procedure:**

- 1.0 Maintenance: The I.T. Manager is responsible for the day-to-day running, control and maintenance of the computer network system. This responsibility may be delegated as needed. Email notifications have been enabled on the firewall as well as syslog messaging. Email notifications and logging are reviewed monthly.
- 2.0 Backups: Daily incremental backups occur for all critical systems on a five day, five week rotation, with monthly backups kept for one year. Day five and month end backups are kept in a fireproof environment onsite. Previous week's tapes are kept offsite in a secured fireproof box at a road commission yard located over five miles away.
- 3.0 Security: All servers are located within a locked server room beyond the doors of a locked office. The Senior Systems Analyst, Managing Director, Finance Director and Maintenance Supervisor are the only four employees with access. Upon termination, keys to the server room are retrieved from terminated employee with access to this area.
  - 3.1 User network access utilizes Active Directory authentication controls. Strong, complex passwords are enforced. Outside network access pertains to the Exchange mail server only; unsuccessful time-outs for users are set to five.
  - 3.2 A new user access form (or access change) is initiated by HR and provided to I.T.; required network permissions are confirmed with supervisor prior to granting employee access
  - 3.3 I.T. is immediately notified of an employee's termination and a user access termination form is completed, disabling access immediately.
- 4.0 Virus Control: MX Records are directed through AppRiver, Inc. where they are scanned for viruses and spam prior to touching the organizational Exchange Server. Symantec mail Security for Exchange is also setup for redundancy in anti-spam and

 <b>ISO 9001-2008 PROCEDURE</b>	<b>PROCESS OWNER</b> Information Technology Management			
<b>PROCEDURE TITLE:</b> Infrastructure - Technology	DOCUMENT NUMBER: ISO_6-3b	REVISION LEVEL: Final Draft	REVISION DATE: 04/20/09	Approval: Managing Director

virus protection as well as content enforcement. Symantec Enterprise Solution is installed on all servers; it is configured to check for new definitions every hour and automatically push out new definitions to workstations.

- 5.0 Environmental Controls: Located on the second floor, servers are protected from water damage. Uninterruptible Power Supplies maintain power for critical servers and network infrastructure for a minimum of 60 minutes; Generators maintain power for servers and air conditioning in the event of a commercial power outage. The dedicated a/c unit keeps the controls at approximately 66 degrees with an alarm in the event temperature exceeds 69 degrees.