BACKUP AND RECOVERY POLICY

Policy Category:	IT
Policy Name:	Backup and Recovery Policy
Version:	1.0
Effective Date:	1-August-2015

Version History

#	Description of Change	Date of Release	**Version No.**	Approved by
1	Release	1-August-2015	1.0	Lalit Jain

Objective:

- Minimize the threat posed by the potential loss or corruption of electronic information owned by the CresTech

Policy Statement:

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Guidelines:

Backup refers to the process of copying data and application files to another physical media to avoid loss of data, and to facilitate recovery, in the event of a system crash. The organization guidelines to ensure secure backups are as follows:

- The information owner must have a documented, communicated, and proven backup/recovery plan in place.
- Backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site.
- Backup medium must be secured during unattended backups, and after completing the backup.
- The media must remain secure until it is erased or destroyed or until the information is reviewed or declassified.
- Information recovery rights must be limited to authorized information custodians. If the information custodian system allows information recovery by information users, recovery access must be limited to the information owner, and authorized information users.
- Recovered information must retain access controls, and ownership consistent with the pre-backup state.
- Recovered information must be inspected for programmed threats, such as viruses, macros, Trojans, that may have been stored in the backup or triggered in the recovery process.
- Information owners must define retention schedule or the criteria for continued value and usefulness.