Policy #: IT.011– Data Protection from Unauthorized Access

Governed by: IT Administration
Approval Date: November 1, 2016 **Last Updated:** November 1, 2016
Purpose: Protection of Data from Unauthorized Access

CEO Data Protection from Unauthorized Access

In order to ensure that data is secured from unauthorized access, we must enforce:

- Password controls must be implemented as per the Password Control and Policy, part of the IT Policy.
- System password details are recorded by IT and kept securely.
- Password Protected Screen Savers may be used when PC/Laptop is idle and unattended.
- Users must lock their PC/Laptop when leaving their desk.
- Monitors used in public areas should be tilted away from the public's direct line of sight so that confidential information cannot be viewed.
- Reports containing sensitive information (e.g. Payroll data) which require disposal should be placed in disposal bags for shredding as confidential waste.
- Secured USB disks should be used when transferring data to outside organizations (which must be provided by the IT Department). Personal USB shall not be used to ensure data integrity.
- All storage media, including backups, should be clearly marked to avoid confusion over their contents.
- Where appropriate; physical controls should be used to prevent unauthorized access.